MELINDA HAAG (CABN 132612)
United States Attorney

J. DOUGLAS WILSON (DCBN 412811)
Chief, Criminal Division

KYLE F. WALDINGER (ILBN 6238304)
MATTHEW A. PARRELLA (NYBN 2040855)
Assistant United States Attorneys

450 Golden Gate Ave., Box 36055
San Francisco, California 94102
Telephone: (415) 436-7200
Fax: (415) 436-7234
E-Mail: kyle.waldinger@usdoj.gov
matthew.parrella@usdoj.gov

JENNY C. ELLICKSON (DCBN 489905)
Trial Attorney

U.S. Department of Justice
1301 New York Avenue., Suite 600
Washington, DC 20530
Telephone: (202) 305-1674
Fax: (202) 514-6113
E-mail: jenny.ellickson@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DAVID NOSAL, Defendant.	No. CR 08-0237 EMC **UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION FOR ACQUITTAL UNDER RULE 29** Hrg. Date: August 7, 2013, 3:00 p.m. Court: Hon. Edward M. Chen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES AND RULES

INTRODUCTION

After a two-week jury trial, the defendant David Nosal was convicted of all of the counts in the Second Superseding Indictment charging him with conspiracy, unauthorized access to a protected computer, and trade secret offenses. On June 14, 2013, he filed a Motion for Acquittal under Rule 29. The United States now files this Opposition. For the reasons stated herein, the defendant's Rule 29 Motion should be denied in its entirety.

THE EVIDENCE AT TRIAL

This section provides a brief summary of trial evidence that relates to the defendant's Rule 29 motion, as well as to his Rule 33 motion; it does not attempt to describe all of the evidence adduced at trial. Additional facts supporting the government's responses to the defendant's arguments are also set out in the relevant sections of this Opposition.

I. AUTHORIZATION TO ACCESS KORN/FERRY'S COMPUTER SYSTEM.

The victim company in this case, Korn/Ferry International ("Korn/Ferry"), is an executive search firm headquartered in Los Angeles, with offices in the Bay Area. Korn/Ferry restricted access to its computer system, including to a database of executives called "Searcher," to users with valid usernames and passwords. Reporter's Transcript ("RT") 567:4–10 & 570:20–23. Korn/Ferry issued usernames and passwords to its employees and, sometimes, to independent contractors. RT 295:7–8, 304:12–14 & 345:9–14. Korn/Ferry prohibited its employees from sharing usernames and passwords with others and expressly warned that the "[u]se of usernames or passwords by unauthorized employees, contractors or guests" could result in criminal prosecution or disciplinary action. RT 563:4–10; Government Trial Exhibit ("GX") 1; *see also* RT 569:10–12 (impermissible for employees to loan credentials to non-employees). The same restrictions applied to both on-site and remote access to the Korn/Ferry computer system. RT 592:5–18. Furthermore, when someone attempted to log into the Korn/Ferry computer system, she would be presented with a banner informing her that she needed "specific authority" to access that system. RT 565–66; GX 5. In addition, when someone on the Korn/Ferry computer system attempted to use Searcher's "custom report" product, she was informed that that product was "intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." GX 2, at

7; *see also* RT 610:2–18.[1]

The defendant was employed at Korn/Ferry from 1996 through October 2004, at which time he entered into an independent contractor agreement with the company. GX 9. Korn/Ferry terminated the defendant's username and password on December 8, 2004. RT 408:19–409:3, 421:2–9 & 571:22–572:9. After that point, the defendant was not authorized to access Korn/Ferry's computer system. RT 408:19–411:2 & 571:22–572:9. The defendant asked for continued access to his Korn/Ferry e-mail and voice mail through the end of 2004, but Korn/Ferry's General Counsel Peter Dunn refused to grant him access. RT 409–10; GX 200. Accordingly, when the defendant needed materials from Korn/Ferry's computer systems for his work on open searches, he could not access the computer system himself and instead needed to ask a current Korn/Ferry employee to provide him with those materials, which Korn/Ferry allowed him to do. *See, e.g.*, RT474:12–16. After his own username and password were terminated in December 8, 2004, the defendant never asked Korn/Ferry to reinstate his access privileges. RT 410:15–21 & 504:22–24.

The cooperating witnesses Becky Christian ("Christian" or "BC") and Mark Jacobson ("Jacobson" or "MJ") were employed at Korn/Ferry with the defendant. Korn/Ferry deactivated BC's and MJ's usernames and passwords after they left Korn/Ferry in January 2005 and March 2005, respectively. RT 573:5–574:18. The defendant never asked Korn/Ferry to reinstate either BC's or MJ's access privileges so that they could assist him with searches he was doing for Korn/Ferry as an independent contractor. RT 410:22–24 & 411:18–22.

By contrast, Korn/Ferry had authorized Jacqueline Froehlich-L'Heureaux ("JFL") to access its computer systems at the time of each of the intrusions charged in Counts Two through Four. RT 574–75. However, JFL was subject to Korn/Ferry's prohibition on sharing usernames and passwords. *See* RT 569:10–12. Korn/Ferry also did not give JFL permission to bestow authorization on someone else by giving her password to them. *See, e.g.*, RT 511:5–9 & 575:4–8.

[1] Custom reports were created during each of the charged April and July intrusions into Korn/Ferry's computer system. *See* GXs 25 & 26; RT 647:2–20, 689:21–25 & 701:16–22.

II. PLANS FOR A NEW SEARCH FIRM.

In mid-2004, while still employed at Korn/Ferry, Nosal became "furious" at Korn/Ferry for appointing Bob Damon, rather than Nosal, to be the president of Korn/Ferry North America. RT 928:21–931:5. Nosal began to have meetings with BC, JFL, and MJ about his plans to leave Korn/Ferry and his desire to start his own business. RT 928:17–20, 929:24–930:10, 931:14–22 & 1097:20–1098:24. In May 2004, during a discussion with Nosal and JFL, BC said that they could take information with them from Korn/Ferry. RT 1284:4–1285:10. Nosal responded, "Don't talk about this in front of me. I don't want to hear it. Talk about it among yourselves." RT 1285:2–4. He did not, however, tell BC and JFL not to take anything from Korn/Ferry. RT 1285:5–10. This subject of taking data from Korn/Ferry came up again within a few weeks, and Nosal again said that he did not want to be part of the discussion and told BC and JFL to figure it out themselves. RT 1285:11–21. During a later conversation between Nosal, BC, and JFL, JFL asked where she was supposed to store Korn/Ferry data, and Nosal told her, "Figure it out; do what you think is best" and gave her his personal credit card. RT 1286:5–17. JFL used the credit card to order two zip drives, one for her and one for BC. RT 1287:5–9; *see* GXs 131 & 157.

JFL understood from these conversations that Nosal wanted her and BC to download materials from Korn/Ferry's computer system. RT 1292:13–19. BC also recalled discussions about obtaining materials from Korn/Ferry's computer system — as BC testified, these were "what was needed and whatever it took kind of discussions." RT 932:8–13. Although BC could not recall exactly what Nosal said, he was "very forceful and directive," and she understood that he wanted her to obtain source lists from Nosal's prior searches at Korn/Ferry that would be helpful to his new business. RT 933:1–12. Nosal, BC, JFL, and MJ also had "team meetings" about this new business at least once a month. RT 1103:17–1104:1. During these meetings, they discussed "a number of different things that [they] would need to launch the business successfully and be ready to go when Mr. Nosal said the doors would open." RT 1104:2–4. MJ understood from these meetings and his conversations with Nosal that Nosal was giving him instructions to bring various types of information over from Korn/Ferry. RT 1105:6–15 & 1202:18–1203:24.

The defendant left Korn/Ferry in late October 2004, and at the encouragement of the

defendant, BC also left Korn/Ferry in early 2005. RT 935:10–936:15. Before she left, however, she took source lists from Korn/Ferry that pertained to "many prominent searches that Korn/Ferry was involved in," not just searches that Nosal himself had conducted. RT 936:16–937:1. BC printed some of these source lists out, and she saved others to a thumb drive, which she later transferred to a CD and to a laptop computer in her home. RT 938:6–939:3. The defendant had asked BC to take these materials because he wanted to use them "to start and/or populate a new database search firm for his benefit." RT 937:2–8; *see also* RT 1049:2 ("Mr. Nosal directed me to take information from Korn/Ferry"). In December 2004, Nosal also purchased a Cluen Corporation software program for such a database. RT 937:9–12. He asked BC to give him the source lists she had taken from Korn/Ferry "pretty soon after he was putting all the pieces together for his new business" and also when he realized that BC was ending their romantic relationship. RT 949:10–16. Nosal referred to these source lists as "his" and asked BC to give them to Michael Louie, whom Nosal planned to hire as the IT person for his company, so that Louie could use the source lists to populate the Cluen database. RT 949:17–950:13.

After BC left Korn/Ferry, Nosal instructed BC to set up a business, Christian & Associates, that would enable him to do his own search work outside of Korn/Ferry. RT 940:24–941:14. Nosal and BC agreed that BC would conduct search work and help Nosal with his searches, and that Nosal would receive eighty percent of any fees, while BC would receive twenty percent. RT 941:15–21. Their clients in this work were billed through Christian & Associates, and JFL, who was still employed at Korn/Ferry, helped BC with the billing. RT 941:22–942:6. Nosal and BC did a significant amount of search work together in the first part of 2005, for which Nosal earned hundreds of thousands of dollars. RT 942:7–945:13. In conducting these searches, BC used the materials she had taken with her from Korn/Ferry. RT 949:1–9. Nosal also used the name "David Nelson" when he and BC interviewed some candidates, and at the defendant's request, JFL used the name "Shelly" when she dealt with candidates or companies that Christian & Associates was working on. RT 952:11–953:20; *see also* RT 1112:11–1113:7 (testimony by MJ about Nosal referring to himself as "David Nelson" on a call with candidate).

As for MJ, he told Nosal in July 2004 that he planned to leave Korn/Ferry to accept an

offer to work for a different firm. RT 1100:6–1101:8. Nosal responded by telling MJ about his plans to start his own search firm and said that BC and JFL were the only other people who knew about these plans. RT 1101:9–19. Nosal invited MJ to be a partner at his new search firm and also asked MJ to stay at Korn/Ferry as long as he could, until Nosal was ready to open his business. RT 1101:19–1102:8. In August and September 2004, and again in early 2005, MJ took source lists, resumes, and other materials from Korn/Ferry searches he had worked on, for the purpose of bringing these materials to Nosal's new business. RT 1107:20–1108:19. Some of these items were printed out, and some MJ kept on computer media. RT 1108:21–24. MJ did not tell Nosal, BC, or anyone at Korn/Ferry that he had taken these items. RT 1108:25–1110:8. MJ ultimately left Korn/Ferry on March 1, 2005, intending to join Nosal's new business when it was up and running. RT 1106:5–11. In July 2005, Nosal helped MJ incorporate a new search firm, Jacobson Search Partners, through which Nosal and MJ would do searches pursuant to the same kind of arrangement that Nosal and BC had for Christian & Associates. RT 1115:7–1116:7.

JFL also told Nosal in March 2005 that she wanted to stop working at Korn/Ferry and work somewhere else until November, when Nosal would be able to start his business openly. RT 1310:19–1312:23. Nosal tried to dissuade JFL from leaving Korn/Ferry and offered to pay her "under the table" to help him set up his new business. RT 1313:19–1315:17. At another point, during a conversation with BC and JFL, Nosal also said to JFL, "What are we going to do when you leave Korn/Ferry?" RT 1328:18–23. In June 2005, JFL told Nosal that she did not want to continue working for him, but she changed her mind after Nosal got "teary-eyed" and said that he could not imagine having a new business without her partnering with him. RT 1316:2–22.

In the spring or summer of 2005, Nosal rented and furnished office space in San Francisco for his new business, Nosal Partners. RT 950:8–22 & RT 1139:2–12. During the week of July 12, 2005, Cluen ran a four-day training for Nosal, BC, MJ, JFL, and others so that they could learn how to use the new database. RT 1135:17–1136:7. During the training, while Nosal was present, MJ mentioned that he had source lists from Searcher. RT 1137:11–17. Nosal expressed surprise at the amount of information MJ had, but he did not tell MJ to get rid of it. RT 1137:21–25. Instead, Nosal put up his hands and said, "We don't have that," which MJ

recognized as "a fairly common response . . . that Mr. Nosal had to various situations over time." RT 1175:17–25. Nosal also said, "I don't want to know about it." RT 1216:10–13. MJ testified that, to him, Nosal's reaction meant that "he knew we had it but he didn't want to kind of acknowledge it." RT 1176:1–11. Nosal also winked at MJ. RT 1176:3–4.

III. OBTAINING INFORMATION FROM KORN/FERRY'S COMPUTER SYSTEM.

The substantive charges in the Indictment were related to thefts from Korn/Ferry's computer system on three dates in 2005. A description of those events is set out below.

April 12, 2005 Downloads

Korn/Ferry's computer logs show that three different source lists were downloaded on April 12, 2005 using JFL's log-in credentials through the Citrix external gateway.[2] *See* RT 762–63; GX 24, at 2. The evidence at trial showed that these source lists were downloaded by BC using JFL's log-in credentials and sent to Nosal. *See* RT 763:24–764:9 & 971:8–972:11; GX 58. The evidence also showed that BC sent Nosal information that she had copied from another source list that day. RT 963:14–964:7 & GX 60.

The information that BC obtained and sent to Nosal was for engagements that they were working on for the companies WorldHeart and UTStarcom. Christian & Associates was retained by WorldHeart on April 12, 2005 to search for a chief financial officer. RT 955–56; GX 138. BC also testified that her company was retained by UTStarcom on April 25, 2005 to search for a chief financial officer for that company, RT 956–57 & GX 56, and that, leading up to that date, she and Nosal had been working to win that business, RT 957–58.

BC and Nosal had discussions about the kinds of information that they needed to obtain for the UTStarcom and WorldHeart engagements. RT 958:8–11.

BC explained to the jury that WorldHeart was in the "medical device space," which was "complicated" and an industry with which neither Nosal nor BC had familiarity. Thus, Nosal needed "help." RT 954:19–21 & 958:15–959:6. BC objected to doing the search because it was

---

[2] Marlene Briski testified that Citrix was software that enabled Korn/Ferry employees to remotely access the Korn/Ferry computer system. RT 590:13–16.

going to be "difficult" and "very hard to conduct." RT 959:7–12. With respect to this engagement, Nosal asked BC "to use searches that Korn/Ferry had done in their database, to find candidates for him that he could quickly call." RT 959:19–25. Nosal and BC stood to gain a total of $66,000 from the WorldHeart engagement. *See* RT 980:19–981:4; GX 138, at 2.

With respect to the UTStarcom search, BC testified that Nosal was "very instructive" about "what searches that he had done or what searches from the source list that could be retrieved." RT 958:12–17. UTStarcom's business was in the "hardware telecom arena." RT 976:6–8. Accordingly, Nosal told BC that "he would need source lists from prior hardware semiconductor-type telecom searches that he or Korn/Ferry had previously done" in order to "quicken and prepare" for trying to get the UTStarcom engagement. RT 960:8–13. Nosal instructed her to get information regarding such searches from Korn/Ferry's computer system, telling her to "Get what you need. Get what I need." RT 971:13 & 960:14–15. Nosal and BC stood to gain a total of nearly $175,000 from the UTStarcom engagement. *See* RT 981:5–982:5.

After her discussions with Nosal about the WorldHeart and UTStarcom engagements, BC obtained JFL's Korn/Ferry log-in credentials from her and used them to access Searcher on April 12, 2005. RT 961–63; GX 57.

For the WorldHeart search, BC testified that she looked in Searcher and found an ongoing search engagement being conducted in the medical device or life sciences industry. RT 963:19–964:3. She obtained information from the source list for that engagement regarding individuals "that World Heart may be interested in from a potential candidate perspective" and sent that information to Nosal in two e-mails (GX 60). RT 964:20–22; *see also* RT 966:17–19. The metadata regarding GX 60 from the defendant's computer indicated that both e-mails had been opened and that they were located in the deleted items folder. RT 1405. Briski confirmed that the information in GX 60 was "a cut and paste of a source list for Sirna Therapeutics, which was an active, open engagement in Searcher on April 12th[, 2005]." RT 766:11–767:7. The Sirna Therapeutics engagement started at Korn/Ferry on April 1, 2005, RT 771:13–14, long after Nosal left the company. *See also* RT 770:19–23 (Nosal *not* assigned to Sirna Therapeutics search).

A physical copy of the second e-mail from GX 60 was recovered in a search of BC's

apartment. *See* GX 63; RT 967:18–20. It was covered in the defendant's handwriting, and the notes there indicated that he had used the information from Korn/Ferry's source list to call numerous candidates. RT 968:5–15. BC testified that one of the individuals listed in GX 60/GX 63 was presented as a candidate to World Heart. RT 968:14–970:11.

For the UTStarcom search, BC copied and downloaded three source lists from prior searches for California Micro Devices and PerkinElmer when she accessed Korn/Ferry's computer system on April 12, 2005. RT 972–75. Nosal worked on all three of these searches when he was at Korn/Ferry and got "contact credit" for them. RT 975:16–18. BC e-mailed these source lists to the defendant, explaining in her e-mail what she was attaching. GX 58. Each of these source lists bore the heading "Korn/Ferry Proprietary & Confidential" on the first page. BC explained to the jury that she obtained these particular source lists for the defendant because "[t]hey would be very appropriate for the CFO search for UTStarcom." RT 976:4–5. In addition to listing candidates that would be appropriate for the UTStarcom position, the source lists contained home and cell phone numbers for the candidates, which was "[e]xtraordinarily important." RT 977:9–20. The metadata associated with GX 58 indicated that it had been opened and was located in the deleted items folder of Nosal's computer. RT 1405–06. There was no testimony one way or the other as to whether the attachments to GX 58 had been opened.

One of the spreadsheets attached to the e-mail in GX 58 was recovered during the search of BC's apartment in August 2005. GX 59; RT 528 & 978. There was handwriting on GX 59. BC was not able to say whose handwriting it was, but did testify that it was not hers. RT 978.

July 12, 2005 Downloads

Korn/Ferry's logs showed that someone accessed its computer system on July 12, 2005 using JFL's credentials through an external Citrix connection and took the following actions:

- queries for executives associated with particular job functions in the utilities industry, RT 686:3–688:19;
- the creation of a custom report listing 65 executives associated with particular job functions in the utilities industry, RT 688:20–690:13, GX 26 & GX 43, at 1–2;
- queries for information about several executives, RT 691:14–693:10;
- a query for Korn/Ferry engagements related to mergers and acquisitions in the

utilities industry, which identified three engagements, RT 693:10–694:16; and

- the creation of a report containing the source list for the Duke Energy search, one of the three engagements identified by the query listed above, RT 694:17–695:12, RT 697:16–19 & GX 43, at 3–6.

See also RT 680:18–681:11 (7/12/2005 Citrix connection); GX 42 (queries into Searcher on 7/12/2005). Briski testified that Korn/Ferry was not able to determine at that time the location from which this Citrix connection was initiated. RT 679:25–680:17. Briski testified that neither Nosal, BC, MJ, nor JFL had been assigned to the Duke Energy engagement. RT 701.

On July 12, 2005, there was training in Nosal's new offices regarding the Encore database that he had purchased. Individuals who were planning to join the new firm, including Nosal, were present. RT 982 & 1338–39. At the time, BC was working on a search with Nosal for a Vice President of Corporate Development for PG&E. The engagement had been pending for more than 30 days, and the defendant wanted the search to be completed as quickly as possible. RT 982:25–985:3. Nosal was the person who primarily conducted that search and BC was trying to identify more candidates for him. RT 985:4–9. Nosal and BC stood to gain more than $120,000 from the PG&E engagement. *See* GX 138, at 3 & 5 (3 payments of $43,555).

BC accessed Searcher using JFL's log-in credentials. Although BC did not recall who typed in JFL's password, JFL testified that she "gave" her credentials to BC. RT 1337:3–14. Once logged in, BC conducted the activities summarized above. RT 985:10–986:9. She testified that GX 44, which was found in her apartment, represented a list of executives in the utilities industry with "functional expertise" in areas such as mergers and acquisitions, corporate planning, and corporate development that she had obtained on July 12, 2005. RT986:14–987:13. The list contained fields for the executives' cell, home, and direct telephone numbers. RT 989:5–8. BC later provided this list of executives to the defendant. RT 987:22–23. BC also testified that it was possible that she also obtained source lists that day that might have been relevant to the PG&E engagement. RT 987:24–988:3. Finally, BC testified that she obtained information from Searcher on July 12, 2005 regarding the CFO engagement for UTStarcom. In this regard, BC testified that Nosal, who was "very frustrated that day, and generally demanding," "yelled at" her because he "needed the cell phone number" of one of the UTStarcom candidates. Nosal asked her

to get that number, and she got it from Searcher. RT 988:9–23.

July 29, 2005 Downloads

Korn/Ferry's logs showed that on July 29, 2005 someone logged into Korn/Ferry's computer system through the Citrix gateway using JFL's credentials and proceeded to download 25 custom reports of source lists. RT 701, 739 & 745; GX 47. On that date, Korn/Ferry was able to determine the Internet Protocol ("IP") address from which that connection originated. From public records searches, Korn/Ferry obtained evidence that the originating IP address was associated with a "Nosal DSL" account. RT 739–41.

Both JFL and MJ testified about July 29, 2005. MJ asked JFL to log in to Korn/Ferry's computer system, which she did, using her own user name and password. RT 1140:6–12, 1141:11–16 & 1339–40. MJ testified that he had downloaded the Citrix software from the Web immediately prior to JFL's log-in. RT 1140–41. MJ asked JFL for her username and password because he did not have access into the Korn/Ferry system. RT 1141:12–13. MJ testified that, thereafter, he ran a number of searches within the Searcher database. RT 1143:13–16. JFL ran no searches that day, nor would she have known how to download source lists. RT 1340:5–9. MJ said that he took these actions at a time when he was working on a project for a company called either Progressive Suspension or Motorsport Aftermarket Group (MAG). RT 1144:7–11. A "MAG - Pres Progressive Suspension" engagement is listed as one of the searches being done by Christian & Associates. *See* GX 139, at 4. These downloads occurred during a time period when MJ was being paid by the defendant. RT 1176:19-25; 1177:1–14; 1181:22–23. MJ testified that there was no doubt in his mind that the defendant knew that source lists were being obtained from the Searcher database for use in the defendant's new business. RT 1230:2–16.

FBI SA Jon Chinn testified that he analyzed the digital contents of the Dell laptop computer seized at MJ's residence. RT 1392:15–17; GX 203. SA Chinn testified he located on that computer all 25 source lists that the Korn/Ferry audit log indicated had been downloaded. RT 1397:8–21; GX 47. SA Chinn conducted a name-by-name comparison to the audit log and found that each name was also on the Excel spreadsheets contained on GX 203. RT 1398:3–14.

LEGAL STANDARDS GOVERNING A DEFENDANT'S MOTION FOR ACQUITTAL UNDER RULE 29

Rule 29 of the Federal Rules of Criminal Procedure states in pertinent part that "[i]f the jury has returned a guilty verdict, the court may set aside the verdict and enter an acquittal." Fed. R. Crim. P. 29(c)(2). It is well settled that the test for determining whether there is sufficient evidence to overcome a Rule 29 motion is whether, "viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Gonzalez*, 528 F.3d 1207, 1211 (9th Cir. 2008) (citation omitted). In ruling on a Rule 29 motion, a district court must bear in mind that "it is the exclusive function of the jury to determine the credibility of witnesses, resolve evidentiary conflicts, and draw reasonable inferences from proven facts." *United States v. Nelson*, 419 F.2d 1237, 1241 (9th Cir. 1969). All reasonable inferences are drawn in favor of the government. *United States v. Andrino-Carillo*, 63 F.3d 922, 924 (9th Cir. 1995), *cert. denied*, 516 U.S. 1064 (1996). Accordingly, "[t]he hurdle to overturn a jury's conviction based on a sufficiency of the evidence challenge is high." *United States v. Rocha*, 598 F.3d 1144, 1153 (9th Cir. 2010).

SUMMARY OF ARGUMENT

This Court presided over the jury trial, as well as the pretrial motion practice. The Court is, therefore, extremely familiar with the legal issues in this case and the evidence presented at trial. Simply put, the evidence at trial was sufficient on all of the counts of conviction. The defendant's motion for a judgment of acquittal should be denied for all of the following reasons.

First, with respect to each of the substantive computer-intrusion counts, the evidence was overwhelming that neither Nosal nor the co-conspirators Becky Christian and Mark Jacobson had authorization to access Korn/Ferry's computer system in 2005 on April 12 (BC), July 12 (BC), and July 29 (MJ). The defendant's argument regarding Korn/Ferry's supposed "authorization" to Nosal, BC, and MJ relies on case law interpreting the "exceeds authorized access" prong of the Computer Fraud and Abuse Act ("CFAA"), which is not at issue in this case. In tandem with his reliance on the "exceeds authorized access" prong, the defendant ignores the case law regarding the "unauthorized access" prong of the CFAA. He avoids the question of whether Nosal, BC, or

MJ were authorized to access Korn/Ferry's *computers* and attempts to divert the Court's attention to the issue of Korn/Ferry's agreement to give Nosal information from those computers.

Second, there was sufficient evidence from which the jury could conclude that Korn/Ferry's source lists constituted trade secrets, and that the conspirators knew them to be trade secrets, intending or knowing that Korn/Ferry would be injured by the theft of those trade secrets.

Third, there was sufficient evidence for the jury to conclude that Nosal knew of and directed the April and July 2005 downloads conducted by BC and MJ, and that he is therefore liable under an aiding and abetting theory both for the computer intrusion charges in Counts Two through Four and the trade secret charges in Counts Five and Six.

Finally, even assuming that the evidence was insufficient to show Nosal's knowledge and direction of one or more of the April and July incidents, he is liable under a *Pinkerton* theory for his conspirators' substantive crimes in Counts Two through Six. The evidence was overwhelming that the defendant entered into a conspiracy to steal information from Korn/Ferry's computer system in or about May 2004. The intrusions into, and thefts of information from, Korn/Ferry's computer system in April and July 2005 were committed in furtherance of that conspiracy, were within the scope of that conspiracy, and were reasonably foreseeable consequences of the unlawful agreement into which Nosal had entered.

ARGUMENT

I. THERE WAS SUBSTANTIAL EVIDENCE FROM WHICH THE JURY COULD CONCLUDE THAT KORN/FERRY HAD NOT AUTHORIZED NOSAL, CHRISTIAN, OR JACOBSON TO ACCESS ITS COMPUTER SYSTEM, THAT NOSAL WAS A MEMBER OF A CONSPIRACY TO ACCESS THAT COMPUTER SYSTEM WITHOUT AUTHORIZATION, AND THAT NOSAL WAS CRIMINALLY RESPONSIBLE FOR THE COMPUTER INTRUSIONS COMMITTED BY CHRISTIAN AND JACOBSON.

Nosal first argues that he must be acquitted of the counts charging him with gaining unauthorized access to a protected computer (Counts Two through Four) and conspiracy to do so (Count One). Viewing the evidence in the light most favorable to the government, there was relevant evidence from which the jury reasonably could have found that (1) Christian and Jacobson knowingly accessed Korn/Ferry's computer system without authorization and with an intent to defraud on the dates alleged in Counts Two through Four, (2) Nosal knew of and directed

those actions, (3) Nosal conspired to gain unauthorized access to Korn/Ferry's computer system, and (4) Nosal is liable, in any event, for the computer intrusions committed by Christian and Jacobson in Counts Two through Four under a *Pinkerton* theory.

A. "Authorized Access" and "Without Authorization" Under the CFAA.

The Ninth Circuit addressed the meaning and scope of the CFAA's "without authorization" prong in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and this decision should be square one of this Court's analysis of the defendant's CFAA arguments. In *Brekka*, the Ninth Circuit held that the plain language of the CFAA indicates that authorization to use an employer's computer "depends on actions taken by the employer." *Id.* at 1135. In other words, "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" *Id.* at 1133; *accord WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) ("[A]n employee is authorized to access a computer when his employer approves or sanctions his admission to that computer"). Accordingly, a person uses a computer "without authorization" under the CFAA "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Brekka*, 581 F.3d at 1135; *accord JBCHoldings NY LLC v. Pakter*, 2013 WL 1149061, at *5 (S.D.N.Y. Mar. 20, 2013) ("[A]n employee 'accesses a computer without authorization' when he does so without permission to do so."); *Lewis–Burke Assocs., LLC v. Widder*, 725 F. Supp.2d 187, 192–93 (D.D.C. 2010) ("an employer's decision to allow or terminate an employee's authorization is the determining factor as to whether the employee is with or without authorization") (citing *Brekka*). This Court instructed the jury on these legal principles from *Brekka*, *see* Doc. 401, at 36 (Instr. 38), and as set out in more detail in Section I.B, *infra*, there was abundant evidence from which the jury could find that Nosal, BC, and MJ had no authorization to access Korn/Ferry's computers on the dates alleged in Counts Two through Four.

There is also no doubt that the "without authorization" prong of 18 U.S.C. 1030(a)(4) — *i.e.*, the prong charged in Counts Two through Four — is concerned with whether a person is

authorized to access a *computer*, not whether she is authorized to possess *information* that comes from that computer. Specifically, section 1030(a)(4) makes it a crime to "knowingly and with intent to defraud, access[] *a protected computer* without authorization . . . and by means of such conduct further[] the intended fraud and obtain[] anything of value." (emphasis added). Other provisions of the CFAA apply the same approach. For example, section 1030(a)(2) makes it a crime to "intentionally access[] a computer without authorization" and "thereby obtain" certain categories of information described in the statute. In other words, this provision distinguishes between unauthorized access of the computer itself and the obtaining of information, which are separate elements of the offense. *See also* 18 U.S.C. § 1030(e)(6) ("'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer . . ."). In light of this clear and unambiguous statutory language, there is no way to read section 1030(a)(4) in the way Nosal claims it could be read — *i.e.*, as precluding liability for someone who has no authorization to access a computer but is authorized to "procure, receive, and use information" from it. R29 Mtn. at 14. Because the "without authorization" prong is therefore not susceptible to multiple interpretations, the rule of lenity does not "come into play."[3] R29 Mtn., at 14; *Chapman v. United States*, 500 U.S. 453, 463 (1991) (rule of lenity applies only where "there is a grievous ambiguity or uncertainty in the language and structure of [an] Act, such that even after a court has seize[d] every thing from which aid can be derived, it is still left with an ambiguous statute") (internal quotation marks omitted).

Brekka also assumes without discussion that the CFAA's "without authorization" prong addresses a person's authorization to access the computer itself, rather than her authorization to obtain to information from that computer. For example, *Brekka* states that "a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access *the computer in question*." *Brekka*, 581 F.3d at 1133 (emphasis added); *see also id.* ("[A]n employer gives an

---

[3] Although Nosal suggests that the CFAA might be vague as applied to JFL, *see* R29 Mtn., at 18, he "cannot complain of the vagueness of the law as applied to the conduct of others" because his own conduct is clearly proscribed by the statute. *United States v. Williams*, 553 U.S. 285, 304 (2008).

employee 'authorization' to access a company computer when the employer gives the employee permission to use it."); *id.* ("[A] person who 'intentionally accesses a computer without authorization' . . . accesses a computer without permission at all.").[4] The Fourth Circuit has also stated that an employee "accesses a computer 'without authorization' when he gains admission *to a computer* without approval" and that "[t]he CFAA is concerned with the unauthorized access of protected *computers*." *WEC Carolina*, 687 F.3d at 204 (emphases added); *see also Lewis–Burke Assocs.*, 725 F. Supp.2d at 193 ("The CFAA is concerned with access to a *computer* . . . .") (emphasis added); *Dana Ltd. v. American Axle & Mfg. Holdings, Inc.*, 2012 WL 2524008, at *4 (W.D. Mich. June 29, 2012) ("The plain language of the CFAA concerns access to a *computer* . . . .") (emphasis added); *cf. also United States v. Pace*, 314 F.3d 344, 349 (9th Cir. 2002) ("Although a fraudulent scheme may be an element of the crime of wire fraud, it is using wires and causing wires to be used in furtherance of the fraudulent scheme that constitutes the prohibited conduct.").

Although Nosal's Rule 29 brief repeatedly invokes the en banc opinion from this case, *see, e.g.*, R29 Mtn., at 8–9, nothing in that opinion alters the legal principles described above or the plain language of the CFAA. To begin with, the Ninth Circuit explained that its decision "follow[ed] in the path blazed by *Brekka*," 676 F.3d 854, 863 (9th Cir. 2012), and expressed no concerns about any aspect of *Brekka*. More importantly, while *Brekka* addressed the scope of the "without authorization" prong that was actually before the jury, the en banc decision focused on the scope of the "exceeds authorized access" prong, which was not at issue at trial. *See generally Nosal*, 676 F.3d at 856–64. Accordingly, the "narrower interpretation" of the CFAA that Nosal seeks to have this Court apply relates to a method of committing a CFAA violation (exceeding

---

[4] As discussed in this paragraph, *Brekka* does not support the proposition that "[a]uthorization . . . means that a party was permitted by the owner of a computer to obtain the information within it." R29 Mtn., at 9:10–11 (citing *Brekka* as support for this statement); *see also id.* at 2:6–7 (arguing that "persons who downloaded information from Searcher were approved by KFI to obtain that same information"). Indeed, *Brekka*'s discussion of "information" in computer systems was largely confined to its discussion of "exceeds authorized access." *See, e.g.*, *id.* at 1133, 1135.

authorized access) that is not implicated in the counts of conviction.[5] R29 Mtn., at 8:19–28 (relying on *Nosal*'s holding regarding "exceeds authorized access").

Furthermore, although the en banc opinion's discussion of the "without authorization" prong is extremely limited, that discussion is wholly consistent with *Brekka*'s holdings about the scope of this term. Specifically, the en banc court stated that the (now-dismissed) CFAA counts at issue in that appeal "fail[ed] to meet the element of 'without authorization'" because "Nosal's accomplices had permission to access the company database and obtain the information contained within." *Nosal*, 676 F.3d at 864. This analysis of "without authorization" is a direct application of *Brekka*. *See Brekka*, 581 F.3d at 1133 ("[A]n employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it."). Moreover, by referring to "access[ing] the company database" and "obtain[ing] the information contained within" in the conjunctive, the en banc court showed that it understood that, under the CFAA, *accessing a computer* is a separate and distinct concept from *obtaining information stored on that computer*. *See Bruesewitz v. Wyeth LLC*, 131 S. Ct. 1068, 1078 (2011) ("[L]inking independent ideas is the job of a coordinating junction like 'and.'").

For all of these reasons, the law in this circuit allowed the jury to conclude that Nosal, BC, or MJ accessed a Korn/Ferry computer "without authorization" as long as the evidence showed that Korn/Ferry had not given them permission to use the computer on the dates in question.

Finally, to the extent that the defendant's motion is based on the argument that the jury was required to find the circumvention of a technological barrier, *see* R29 Mtn., at 2:2–5, 17–18, this Court already considered and rejected this limitation on "without authorization" in its order denying the defendant's motion to dismiss. *See United States v. Nosal*, 2013 WL 978226, at *8 (N.D. Cal. Mar. 12, 2013); *cf. Weingand v. Harland Fin. Solutions, Inc.*, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012). Nosal has identified no basis for the Court to reconsider this issue.

---

[5] Likewise, to the extent that the en banc court concluded that the CFAA was ambiguous and applied the rule of lenity, it did so only with respect to the term "exceeds authorized access" and did not suggest that the term "without authorization" was subject to multiple interpretations or otherwise ambiguous. *See Nosal*, 676 F.3d at 863.

B. There was Sufficient Evidence for the Jury to Conclude that Nosal, Christian, and Jacobson Were Not Authorized to Access Korn/Ferry's Computer System after They Left Korn/Ferry's Employment, That They Knew They Were Not Authorized, and That They Accessed That Computer System with an Intent to Defraud.

Applying the law set forth above, the jury was presented with sufficient evidence from which it could conclude that Korn/Ferry did not authorize Nosal, BC, or MJ to access its computer system on the dates alleged in the substantive computer intrusion counts in the Indictment. There was also sufficient evidence from which the jury could conclude that those individuals knew that they were unauthorized and acted with an intent to defraud.

1. *There Was Sufficient Evidence for the Jury to Conclude That Only Individuals with Valid Usernames and Passwords Were Authorized to Access Korn/Ferry's Computer System.*

The jury was presented with abundant evidence from which it could conclude that only individuals with usernames and passwords issued by Korn/Ferry were authorized by the company to access its computer system.

Marlene Briski, Korn/Ferry's Vice President of Information Services, testified that Korn/Ferry's Information Technology and Security Policies and Procedures in effect at the time of the intrusions provided that an employee's username and password was "to be used by the intended employee only." RT 563:4–10; GX 1; *see also* RT 569:10–12 (impermissible to loan usernames and passwords to non-employees). Before logging in, a user was presented with a banner informing her that she needed "*specific* authority" to access Korn/Ferry's computer system. RT 565–66 (emphasis added). Unless the user entered a valid username and password, she could not gain access to the computer system. RT 567:4–10 & 570:20–23.

2. *There Was Sufficient Evidence for the Jury to Conclude That Korn/Ferry De-Authorized Nosal's, Christian's, and Jacobson's Usernames and Passwords and, Thereafter, Did Not Authorize Them to Access its Computer System.*

Peter Dunn, Korn/Ferry's General Counsel, and Briski testified that Nosal's username and password were terminated on December 8, 2004, and that, thereafter, he was not permitted to access Korn/Ferry's computer system. RT 408:19–409:3, 421:2–9 & 571:22–572:9. Indeed, Dunn testified about an incident in which Nosal asked that he be left "on Korn/Ferry email and voice mail until the end of December [2004]." RT 409:19–23; GX 200. Dunn did not consent to

that request. RT 410. Briski also testified that BC's and MJ's usernames and passwords were de-authorized upon the termination of their employment with Korn/Ferry in January 2005 (BC) and March 2005 (MJ). RT 573:5–574:18.

Although Dunn testified that Nosal could ask Korn/Ferry employees to obtain materials for him from Korn/Ferry's computer system regarding the open searches on which he was working, *see, e.g.*, RT 474:12–16, there was absolutely *no testimony* that Nosal, BC, or MJ were allowed to *personally access* the computer system, particularly in light of the computer use policies described above. Dunn was the person who dealt with Nosal after Nosal's departure from Korn/Ferry. He testified that he never gave Nosal authority to access Korn/Ferry's computer system, RT 410:25–411:2, and Nosal never asked that his access privileges be reinstated after they were terminated, RT 410:15–21 & 504:22–24. Nor did Nosal ever ask that any non-Korn/Ferry employees — including BC and MJ — be given access to the computer system to assist him with open searches. RT 410:22–24 & 411:18–22. Even assuming that Nosal himself was "authorized" to access Korn/Ferry's computer system as that term is interpreted under section 1030, he had no authority to confer such authorization to others such as BC and MJ. RT 510:25–511:4.

Not only was there testimony from the owner of the computer that Nosal, BC, and MJ were not authorized to access its computers, but BC and MJ each testified that they had not received Korn/Ferry's permission to access its computer system on the dates in question. *See* RT 976:17–19, 983:17–21 & 1143:8–11. Their understanding that they did not have Korn/Ferry's permission was certainly buttressed by the fact that their intrusions into the computer system in April and July 2005 were not related to Korn/Ferry searches. *See* RT 963:9–13, 983:23–984:4 & 1144:7–11; *see also* RT 1079:13–1080:6 (no need to develop source lists for any Korn/Ferry searches after BC's departure from Korn/Ferry). Indeed, the government believes that there was *no evidence* that MJ was *ever* tasked by Nosal to work on Korn/Ferry search assignments *after* he left Korn/Ferry, *see, e.g.*, RT 1177:6–14 & Defense Exhibit ("DX") E, so it would be strange for him or for anyone to conclude that he was still "authorized" to access Korn/Ferry's computer system. As for BC, she testified that she believed that, as of April 12, 2005, the Korn/Ferry work assignments on which she had been working had been concluded and "transitioned" back to

Korn/Ferry. RT 963:9–13; *see also* RT 484 (Dunn testimony that BC's name on DX E reflected "credit attribution" rather than "working on the assignment").[6]

Furthermore, because Nosal, BC, and MJ were all former Korn/Ferry employees who had used Korn/Ferry computers during their employment, the jury reasonably could conclude that they knew they were not authorized to access those computers unless Korn/Ferry gave them "specific authority" to do so, particularly in light of Korn/Ferry's clear desire to protect the information in its database from outsiders. GX 5 (banner on Korn/Ferry computers); *see, e.g.*, GX 7; GX 8, §§ 5.A & 5.B, at 5–6; GX 9, § 18, at 9; GX 15, at 3. The jury could also conclude that Nosal, BC, and MJ were familiar with Korn/Ferry's policies regarding usernames and passwords, *see* GX 1, and therefore knew that JFL was not allowed to share her password with them at all, much less bestow authorization on someone by giving her password to them. *See, e.g.*, RT 511:5–9 & 575:4–8. The defendant's suggestion, therefore, that JFL's actions in allowing BC and MJ to use her password take this case out of the "ambit of the CFAA," R29 Mtn., at 12:27–13:1; *see also id.* at 2:5 ("consent of [] the password holder), ignores the evidence presented at trial and the plain language of *Brekka* and *Nosal*.[7]

/ / /

---

[6] Nosal's argument that Dunn "never told [Nosal] that BC and MJ could not continue to work" on searches after they left Korn/Ferry, *see* R29 Mtn., at 11:7 (apparently relying on RT 491), demonstrates only that Dunn was unaware that Nosal might have BC and MJ do so. *See, e.g.*, RT 479:22–24. For these reasons, and for all of the reasons set forth in the text above, Nosal's statement that "KFI agreed that BC and MJ could continue working on his behalf for open searches, and there is *no evidence* that KFI ever rescinded that agreement," R29 Mtn., at 11:11–12 (emphasis added), is contrary to the standards that this Court must apply to a Rule 29 motion because it draws all reasonable inferences *against* the government.

[7] The defendant contends that the government "conceded" that "giving another person one's password in itself does not violate the CFAA." R29 Mtn., at 13:6–8. Of course, the government's decision to dismiss password trafficking as an object of the charged conspiracy does not amount to a "concession." The government's decision came after much discussion of the password trafficking issue before the Court. *See* RT 1457–62 & 1472–73. In any event, as the government pointed out, including password trafficking (a misdemeanor) as an object of the conspiracy raised issues regarding the verdict form, which issues were resolved by dropping it as an object. *See* RT 1536:11–25.

3. *The Conspirators' Actions Are Consistent with the Conclusion That Nosal, BC, and MJ Were Not Authorized to Access Korn/Ferry's Computer System; the Conspirators' Actions Also Evince Knowledge and an Intent to Defraud.*

In reaching its conclusion that Nosal, BC, and MJ were not authorized to access Korn/Ferry's computer system, and knew so, the jury also could have relied on the fact that each of them *acted consistently* with not having been given such authorization. For example, knowing that his request to keep his Korn/Ferry e-mail and voice mail had been denied, Nosal never asked Peter Dunn to provide BC and MJ with usernames and passwords. RT 410:22–24 & 411:18–22. Furthermore, when BC and MJ e-mailed JFL to ask her for her log-in credentials or for information from Korn/Ferry's computer system for one of the non-Korn/Ferry searches on which they were working, they sent those e-mails to her Yahoo or Hotmail address, not her Korn/Ferry e-mail address. *See, e.g.*, GXs 27, 57 & 79. Nosal also communicated with JFL through her personal e-mail address. *See, e.g.*, GX 79. In light of these attempts to avoid detection, the jury reasonably could conclude that Nosal, BC, and MJ knew that they were not authorized to access Korn/Ferry's computers and were accessing those computers with intent to defraud.[8]

The jury also saw evidence that another member of the conspiracy — JFL — made efforts to keep her actions concealed from Korn/Ferry, such as by initiating e-mail communications from her Yahoo or Hotmail address. *See* GXs 29 & 50. JFL was also concerned about whether Korn/Ferry could trace her computer connection from Nosal's new offices. RT 1265. And, in providing materials from Korn/Ferry's computer system to the other conspirators, JFL adopted naming conventions intended to disguise the nature of those materials. *See, e.g.*, GX 71, at 4 ("Chocolate Chip Cookie Recipes.doc" and "Invitation to Marcy's Bridal Shower.doc"); RT 668–69 ("choc chip cookie recipes"). If Korn/Ferry had authorized Nosal, BC, and MJ to access its computer system, then there should not have been a reason for JFL to have taken these actions

[8] There was abundant other evidence of the conspirators' intent to defraud in this case, including their agreement at the outset of the conspiracy to steal information from Korn/Ferry; Nosal's desire to have JFL continue to work at Korn/Ferry, RT 1313–14 & 1328:18–23; and Nosal's concealment from Peter Dunn that he was doing work for non-Korn/Ferry clients and obtaining materials from Korn/Ferry's system regarding non-Korn/Ferry searches, RT 411.

or to express these concerns. And, again, the use of these naming conventions is a reflection of the conspiratorial agreement to defraud Korn/Ferry of its property.

* * *

Nosal's arguments pertaining to his, BC's, and MJ's ongoing authorization to access Korn/Ferry's computer system, *see, e.g.*, R29 Mtn., at 10:22–11:18, ignore all of the evidence set out above. Instead, he focuses on Korn/Ferry employees' decisions in other circumstances to provide Nosal and BC with particular documents. *See, e.g.*, R29 Mtn., at 11:8–9. Based on the law set forth in Section I.A, *supra*, these arguments are without merit because the CFAA is concerned with access to a *computer*, not simply to data that may have come from a computer.

C. There Was Sufficient Evidence for the Jury to Conclude that Nosal Knew of, Directed, and Conspired to Commit the April and July Downloads from Korn/Ferry's Computer System.

As set forth in more detail below, there was sufficient evidence upon which the jury could have concluded that Nosal knew of, directed, and conspired to commit the April and July downloads by Christian and Jacobson.

1. *April 12, 2005 Downloads*

The evidence at trial showed that BC used JFL's username and password to download three source lists from Searcher on April 12, 2005, and that she then e-mailed those source lists to the defendant. GX 58. These source lists were from CFO search engagements for California Micro Devices and PerkinElmer that Nosal had worked on when he was employed at Korn/Ferry. RT 975. BC obtained these three source lists for the purpose of assisting Nosal regarding a CFO engagement for UTStarcom. RT 971. Also on April 12, 2005, BC "cut and pasted" information from a source list in Searcher related to an ongoing Korn/Ferry search for Sirna Therapeutics and sent that information in two e-mails to Nosal. BC obtained this information for the purpose of assisting Nosal regarding a CFO engagement for WorldHeart. *See* RT 963:14–964:7; GX 60.

For the reasons set forth in Section I.B, there was sufficient evidence for the jury to conclude that this intrusion was unauthorized, that Nosal and BC knew that the intrusion was unauthorized, and that the intrusion was performed with the intent to defraud. There is no serious dispute that "something of value" was obtained by virtue of the intrusion.

Nosal argues that the jury could not have reasonably concluded that he knew that there would be an intrusion into Korn/Ferry's computer system by someone other than JFL. R29 Mtn., at 15:25–27. However, taking the evidence in the light most favorable to the government, the jury reasonably could have concluded that Nosal asked BC to personally obtain information from Searcher on April 12, 2005, that he knew that she would be the person engaged in the intrusion, and that he conspired with her on or before that date to gain unauthorized access to Korn/Ferry's computer system. For example, the jury was presented with evidence that Nosal had asked *Christian* (not JFL) to get the information. *See, e.g.*, RT 971:13 ("Get what you need. Get what I need."). In addition, there was other evidence upon which the jury could rely to conclude that Nosal knew that BC would be performing the queries herself. BC testified that during the time she worked with Nosal at Korn/Ferry, he had relied on *her* to obtain information from Korn/Ferry's computer system on a "daily" basis. RT 921:15–18. BC also testified that she worked closely with Nosal and shared with him what she was doing in her work life, which included brainstorming with him about what source lists to look at, and telling him what source lists she was looking at. RT 925:11–926:6. During the period at issue, BC saw Nosal on a daily basis, and she and Nosal did work together at her home. RT 926:7–19.

Based on these facts and the facts set forth in "The Evidence at Trial" Section, the jury would have been justified in placing weight on BC's testimony that Nosal knew that she was using JFL's password to get materials from Korn/Ferry's computer system. RT 1081. This is especially so in light of the fact that JFL testified that she "never" ran a custom report of source lists, "never" pulled an old source list, and did not know how to do so. RT 1279–80. Given Nosal's long association with Christian (since 1999) and JFL (since 1997), he therefore knew that obtaining source lists would be a task that would be accomplished by Christian, not by JFL.

In addition to the evidence set forth above showing that Nosal knew that BC would be obtaining information from Searcher, the jury was also presented with evidence showing that Nosal (1) wanted that information quickly, (2) put the information that he obtained to use, and (3) stood to gain significant amounts of money from the engagements at issue. As set out below, this evidence supports the conclusion that Nosal knew how the information would be obtained.

For example, there was abundant testimony that Nosal wanted the tasks that he had directed BC to do to be done expeditiously. In her testimony, Christian used variants of the word "quick" no less than 10 times to describe the importance that Nosal placed on speed in executing searches, and the difficulty in doing so. *See* RT 921:11, 933:7, 954:5–6, 954:14, 959:25, 960:13, 961:8, 984:22, 985:2; *see also* RT 921:5–6 ("[Nosal] was interested in leveraging names from prior searches in order to help expedite a current search.").

The jury was also presented with substantial evidence showing the utility to Nosal of the information that BC obtained from Searcher. For example, at least three people whose names were set forth in the source lists attached to the e-mail in GX 58 were later presented to UTStarcom as possible candidates for its CFO position. RT 979:4–980:3. Similar evidence was presented with respect to one of the individuals listed in GX 63. *See* GX 64 (presentation of circled name on GX 63); RT 968–70. Nosal himself underlined for the jury the importance he placed on the information that he had obtained from Korn/Ferry because GX 63 was covered in his handwriting. Moreover, BC sent Nosal source lists containing "extraordinarily important" non-public contact information for the candidates, and BC testified that the *only* place that she could get source lists she had downloaded was from Korn/Ferry. RT 977:18–25.

The jury also had evidence of another motive Nosal had for stealing information from Korn/Ferry: money. "Money was very important to the defendant," RT 948:14–15, and he and BC stood to gain well over $200,000 from the WorldHeart and UTStarcom engagements.

Based on these additional facts showing the importance that Nosal placed on getting information quickly, his use of the information he obtained, and the financial benefits to him, as well as on testimony about the defendant's management style, the jury reasonably could conclude that Nosal knew how BC was going to obtain the information that was so important to him. *See also* RT 932:23–25 ("He's very directive."); *see also* RT 1105–06 (MJ testimony that, although Nosal "didn't necessarily try to micromanage . . . he stayed very close to the details"). Indeed, the testimony at trial showed that Nosal directed minute details of Christian's life. *See, e.g.*, RT 1067:6–25 (BC resignation e-mail dictated in part by Nosal); GX 126 & RT 945:14–948:10 (exhibit and testimony of instructions re: money); RT 969:19–20 ("I was generally not able to

send emails without the defendant's knowledge or instruction . . . ."). Furthermore, after the FBI's execution of the search warrants in August 2005, Nosal never expressed anger at Christian for what she had done. RT 1000:8–13. If Nosal had been unaware of her actions, a more natural reaction would have been for him to express such anger. The jury reasonably could have concluded that he had not because he knew what actions Christian had taken.

2. *July 12, 2005 Downloads*

The testimony at trial also demonstrated that BC used JFL's log-in privileges to obtain various types of information from Korn/Ferry's computer system on July 12, 2005. This information included one source list from a prior Korn/Ferry engagement for Duke Energy, a list of executives who were involved in mergers and acquisitions in the utilities industry, and contact information for a candidate for the UTStarcom CFO search.

For the reasons set forth in Section I.B, there was sufficient evidence for the jury to conclude that this intrusion was unauthorized, Nosal and Christian knew that the intrusion was unauthorized, and the intrusion was performed with the intent to defraud. Again, there is no serious dispute that "something of value" was obtained by virtue of this intrusion.

Nosal argues that there was no evidence that he was informed of the July 12, 2005 intrusion either before or after it happened. There was sufficient evidence for the jury to conclude otherwise. As an initial matter, the jury heard testimony that Nosal had previously directed BC to obtain materials from Searcher in April 2005 when he was faced with similar challenges in executing a search engagement. In addition, BC testified that Nosal was present in his new offices when she committed this intrusion. During the time that she was logged into Korn/Ferry's computer system, Nosal was yelling at her to get a contact number for a candidate for the UTStarcom CFO position. RT 988:9–23. From this, the jury could have concluded that Nosal knew that BC was in Korn/Ferry's database, especially in light of the fact that she appears either to have been sitting at JFL's computer, RT 1245 (Louie testimony), or at the defendant's computer, RT 985:18–24 (BC testimony).

BC also testified that the PG&E search, from which Nosal stood to gain over $120,000, was taking longer than he wanted. The jury could rely on this cash motive, along with the

premium that Nosal placed on speed in the execution of searches, to conclude that he knew the actions that BC was taking to get him the information he needed regarding potential candidates.

Finally, much of the evidence cited above with respect to the April 12, 2005 intrusion applies equally to the July 12, 2005 intrusion. The jury was presented with evidence that Nosal and BC had a close working relationship, and that that relationship had existed since 1999. The jury reasonably could have concluded that, as BC testified, RT 1081, Nosal knew that she was using JFL's password to obtain materials from Searcher. Moreover, the tasks that BC engaged in on July 12, 2005, were ones that JFL apparently did not know how to do, RT 1337:12–16, which Nosal would have known based on his long interaction with her.

For all of these reasons, there was sufficient evidence for the jury to conclude that Nosal knew of and directed BC's actions on July 12, 2005.

3. *July 29, 2005 Downloads*

The evidence at trial showed that Jacobson accessed Korn/Ferry's computer system on July 29, 2005, and downloaded 25 source lists. Again, as set forth in Section I.B, there was sufficient evidence for the jury to conclude that this intrusion was unauthorized, that Nosal and MJ knew that such an intrusion would be unauthorized, the intrusion was performed with the intent to defraud, and that "something of value" was obtained.

The July 29, 2005 access to the Searcher database itself was clearly unauthorized. MJ accessed the Korn/Ferry computer system by taking over at the computer after JFL logged in using her Korn/Ferry credentials. JFL did not have the authority to confer access rights to those not employed by Korn/Ferry. Finally, as the Court indicated in its order of March 12 , 2013 (Doc. 314, at 14–16), "[t]hat J.F. entered the password for him rather than having M.J. type it himself does not alter the fact that in common parlance and in the words of the CFAA, M.J. accessed the protected computer system, and he did not have authorization to do so." The defendant ignores this important part of the Court's prior order and continues to argue as if the mere fact that JFL typed in her Korn/Ferry password was a defense to the July 29, 2005 CFAA counts. It is not.

Although MJ testified that he had not been expressly directed by Nosal to go into Searcher on July 29, 2005, RT 1213, the jury could reasonably conclude that Nosal knew that MJ would

engage in this conduct or was aware of a high probability that he would do so and deliberately avoided learning the truth. Everyone in the scheme — the defendant, BC, MJ, and JFL — knew precisely how that scheme operated, that is: the defendant, with full knowledge that the data he wanted resided on the Korn/Ferry system, directed either BC or MJ to perform executive searches that he similarly knew required access to that Korn/Ferry data. Only JFL had a valid username and password for the Korn/Ferry system, and JFL herself testified that she did not have the technical ability to obtain a source list. The jury reasonably could infer that the defendant's long business relationship with JFL taught him the same thing, leaving only one reasonable path forward for the conspiracy: JFL needed to turn over her Korn/Ferry username and password to BC and MJ, who would then use those credentials to steal Korn/Ferry data to give to the defendant. The stolen data was immediately apparent to the defendant as having originated from Korn/Ferry, if for no other reason than he himself had worked on some of the searches that generated that data while at Korn/Ferry. Viewed in a light most favorable to the verdict, these facts show that the defendant knew that the Korn/Ferry system was being repeatedly accessed without authorization by his underlings' use of JFL's credentials.

The jury also heard testimony from several witnesses that, less than three weeks before these downloads, Nosal and MJ were involved in an incident at Nosal's new offices during which the topic of "Korn/Ferry data" came up. During the training being presented by a Cluen Corporation representative regarding the database program (Encore) that Nosal had purchased, MJ announced that he was in possession of Korn/Ferry data, and referenced "source lists." RT 1137:11–15 & 1228:3–19; *see also* RT 1338:18–19 (JFL: "He said words to the effect of, when I left Korn/Ferry I took copies of everything I had ever worked on there."). MJ testified that Nosal's reaction was that of surprise at the *amount* of data that MJ had. RT 1137:21–21 & 1175:18–22. Representatives from Cluen were in the room, and Nosal then said "we don't have that" or "we don't have Korn/Ferry data," RT 1175:24 & 1271:24–25, although, as MJ said, Nosal "knew we had it but he didn't want to kind of acknowledge it." RT 1176:1–4; *cf.* RT 1339 (JFL: Nosal "immediately said, All of our data belongs to us, to me"); *id.* (noting that both JFL and Nosal were "startled that Mark would blurt something out like that"). Nosal also winked at MJ

during this exchange. RT 1176:3–4. After being told about the volume of data that MJ had taken from Korn/Ferry, Nosal did not instruct him to give the data back.[9] RT 1137:24–1138:3. On the contrary, Nosal simply told him, "I don't want to know about it." RT 1216:13. The jury reasonably could have concluded from Nosal's actions and statements on the day of the Cluen training that he was aware all along that Korn/Ferry data had been and was being obtained by MJ, and that he expected MJ to continue to do so.

The jury also reasonably could have concluded that MJ's actions were in furtherance of his conspiracy with Nosal to obtain information from Korn/Ferry's computer system. As MJ testified at trial, he was working on a project for a company called either Progressive Suspension or Motorsport Aftermarket Group. Based on the evidence that the defendant "stayed very close to the details," RT 1105–06, the jury reasonably could conclude that Nosal knew what steps MJ needed to take in order to execute the search. Moreover, the jury saw evidence that all but 19 of the 25 source lists downloaded by MJ on July 29, 2005 had been from Korn/Ferry searches conducted by Nosal himself. *See* GX 198; RT 750. MJ also testified that there was no doubt in his mind that the defendant knew that source lists were being obtained from the Searcher database for use in the defendant's new business. RT 1230:2–16.

Another sound basis for the jury to infer the defendant's knowledge is that, on a prior occasion, April 12, 2005, the defendant specifically directed BC to obtain data from the Korn/Ferry system at a time when neither he nor BC worked for Korn/Ferry. RT 950:14–19. The defendant later was provided with the results of his directive. These facts establish that the defendant's knowledge going forward from that date was that JFL's credentials would be used by other members of the conspiracy to obtain needed materials from Korn/Ferry's computer system.

/ / /

[9] Indeed, rather than directing that the data be deleted or given back to Korn/Ferry, the evidence showed that Nosal continued with the plan that had been hatched in the summer of 2004 to put that data into his new company's database. RT 1138:21–24; *see also* RT 1172–73 (MJ had discussions with Nosal and others about getting data they had collected from various sources, including Korn/Ferry, into Nosal's new database).

4. *Based on the Evidence Discussed Above Regarding the April and July Intrusions, the Jury Reasonably Could Have Concluded that Nosal Conspired to Commit Unauthorized Access to Korn/Ferry's Computer System.*

For all of the reasons set forth above, the evidence was sufficient to show that Nosal *also* conspired to violate the CFAA. For example, BC was not employed at Korn/Ferry at the time that Nosal instructed her to obtain items from Korn/Ferry's computer system in April 2005. Accordingly, even though BC's downloads during their employment may not have given rise to CFAA liability, *see* R29 Mtn., at 10:1–21, there was sufficient evidence to support the conclusion that Nosal did conspire to gain unauthorized access to Korn/Ferry's computer system based on the events in April 2005.

5. *The Fact that Korn/Ferry was Monitoring the Intrusions on July 12 and July 29 Does Not Require Acquittal on Those Counts.*

The defendant's final argument with regard to the CFAA convictions is that he must be acquitted of Counts Three and Four because BC's and MJ's intrusions into Korn/Ferry's computer system on the relevant dates "were made with the full knowledge of KFI, which was monitoring the entries and could have easily prevented them." R29 Mtn., at 18:15–16. This argument fails for several reasons. As an initial matter, it is well-settled that individuals may be convicted of criminal conduct, even when it is done under the watchful eyes of law enforcement or other entities that could prevent the activity. *See, e.g.*, *United States v. Ramirez*, 714 F.3d 1134 (9th Cir. 2013) (upholding defendant's convictions for distribution and possession with intent to distribute methamphetamine after undercover agent purchased drugs from defendant four separate times). Indeed, once Korn/Ferry discovered that it was the victim of an ongoing criminal scheme, it would have been wholly appropriate for Korn/Ferry to "smooth[] the way for the commission of the crime in order that the criminal might be apprehended." *Smith v. United States*, 291 F.2d 220, 221 (9th Cir. 1961) (noting, in bank robbery case, that the bank "was under no duty to prevent the crime nor place obstacles in the way of its commission"). Moreover, Korn/Ferry employees never had personal knowledge as to whether someone other than JFL accessed the company's computer system on July 12 and July 29 because those intrusions occurred within Nosal's offices. (As to the July 12 incident, Briski testified that Korn/Ferry did not even know at that time from where

the intrusion originated. RT 679:25–680:17.) In any event, the defendant's interpretation of the statute would mean that unauthorized access crimes could not be prosecuted where the victim computer owner discovered that someone may have accessed its computer without permission and stolen things of value and then took reasonable steps to investigate the intrusion in order to determine *who* had committed the crime and *where* the stolen materials had gone. As the United States noted in response to the defendant's motion to dismiss, the argument that Korn/Ferry's investigation itself somehow conferred authorization for the very criminal actions forming the basis of that investigation stands logic on its head.[10]

D. The Agreement in 2004 to Steal Information from Korn/Ferry Supports Application of the *Pinkerton* Doctrine to the Substantive Computer Intrusion Charges in Counts Two Through Four.

The defendant makes only a fleeting mention of the *Pinkerton* doctrine. *See* R29 Mtn., at 10 & 16. Understandably so. The evidence at trial showed that Nosal entered into a conspiracy in approximately May 2004 to steal trade secrets and other information from Korn/Ferry's computer system. The evidence of this agreement was overwhelming. BC, MJ, and JFL testified that they made surreptitious plans with Nosal to take trade secrets in the form of source lists and other confidential information from Korn/Ferry. The jury was presented with a physical manifestation of these plans — the "zip" drive that Nosal instructed JFL to purchase with his personal credit card, as opposed to his Korn/Ferry's Diners Club card. *See* GXs 131 & 157; RT 1286:15–16 ("he did tell me not to use his Korn/Ferry Diners Club") & 1292 (use of Nosal's *non*-Korn/Ferry e-mail address to order "zip" drives). Even after Nosal, BC, and MJ left Korn/Ferry's employment, the evidence showed that Nosal directed that additional information be obtained from Korn/Ferry's computer system. *See, e.g.*, Section I.C.1, *supra*.

Nosal's participation in this conspiracy to steal information belonging to Korn/Ferry in

---

[10] In fact, 18 U.S.C. § 2511(2)(i)(I-IV), the so-called "hacker's exception" to the wiretap statute declares that it is not unlawful to intercept the communications of a "computer trespasser" when, among other requirements, "the person acting under color of law is lawfully engaged in an investigation." This statute's underlying assumption is that an investigation into an ongoing intrusion does not confer authorization for that very intrusion.

violation of the trade secret statute means that he may be convicted for the substantive crimes committed thereafter by his co-conspirators under a *Pinkerton* theory, even if the evidence was not sufficient to find him liable under an aiding and abetting theory. *See United States v. Alvarez-Valenzuela*, 231 F.3d 1198, 1202–03 (9th Cir. 2000); *see also United States v. Nakai*, 413 F.3d 1019, 1023 (9th Cir.), *cert. denied*, 546 U.S. 995 (2005) (*Pinkerton* theory "broadens a defendant's liability beyond the aiding and abetting charge implicit in any indictment").

First, as discussed in the previous subsections, the evidence showed that BC and MJ committed substantive CFAA offenses in April and July 2005.

Second, the government proved that the defendant was a member of the conspiracy when the substantive offenses were committed. The evidence showed that a conspiracy began in May 2004 to steal information from Korn/Ferry's computer system, and that that conspiracy continued until at least July 29, 2005. Once started, the agreement is presumed to continue until there is abandonment or withdrawal. *See United States v. Jimenez Recio*, 537 U.S 270, 274–75 (2003). The burden for establishing withdrawal is placed on the defendant. *Smith v. United States*, 133 S. Ct. 714, 719 (2003).

Third, the government showed that the substantive offenses were committed in furtherance of the conspiracy to steal information to be used in Nosal's own executive search activities.

Fourth, the computer intrusions were a reasonably foreseeable consequence of the unlawful agreement and were within the scope of the agreement. Nosal and BC worked hand in hand on the engagements to which BC's intrusions related, and the jury heard evidence that the defendant actively participated in the conspiracy to steal Korn/Ferry information. For example, as set forth in Section I.C.1, *supra*, the jury heard considerable testimony from BC regarding her discussions with Nosal about the kinds of information that he needed her to get from Searcher to assist in the UTStarcom and WorldHeart searches. Even if Nosal did not "know" that BC would personally access Searcher based on his instructions, it was reasonably foreseeable that she would do so, given the overall conspiracy to take information from Korn/Ferry. The fact that the conspiracy, as hatched in 2004, may not have had as an object unauthorized access to Korn/Ferry's computer system does not mean that Nosal may not be found guilty of a substantive

offense of unauthorized access under the *Pinkerton* doctrine. *See United States v. Allen*, 425 F.3d 1231, 1234 (9th Cir. 2005) ("The *Pinkerton* rule holds a conspirator criminally liable for the substantive offenses committed by a co-conspirator when they are reasonably foreseeable and committed in furtherance of the conspiracy.") (internal quotation marks omitted); *United States v. Odom*, 13 F.3d 949, 959 (6th Cir. 1994) ("Once a conspiracy is shown to exist, the *Pinkerton* doctrine permits the conviction of one conspirator for the substantive offense of other conspirators committed during and in furtherance of the conspiracy, even if the offense is not an object of the conspiracy."); *cf. United States v. Carter*, 560 F.3d 1107, 1112–13 (9th Cir. 2009) (upholding defendant's conviction, based on *Pinkerton* liability, for use of a firearm during a crime of violence based on his involvement in a conspiracy to commit a bank robbery).

The evidence also showed that Nosal played a substantial role in the conspiracy and, indeed, led and controlled the overall conspiracy. Given Nosal's major, central role in the overall conspiracy, the jury could conclude that he reasonably foresaw that his co-conspirators would take the steps they did to obtain data from Korn/Ferry. *Cf. United States v. Bingham*, 653 F.3d 983, 998 (9th Cir. 2011) ("Hevle's role [in the gang] was neither minor nor marginal; given it, he could reasonably foresee that a co-conspirator might commit murder in furtherance of the conspiracy.").

For these reasons, Nosal's argument that he could not be convicted of a substantive CFAA offense unless there was proof that he joined a "CFAA conspiracy" is without merit. *See* R29 Mtn., at 16:8–10.

II. THE JURY WAS PRESENTED WITH SUFFICIENT EVIDENCE FROM WHICH IT COULD CONCLUDE THAT NOSAL WAS GUILTY OF THE TRADE SECRET CHARGES.

At the outset of his discussion of the trade secret offenses, the defendant goes to some effort to discuss the law of trade secrets and the government's burden of proof with respect to the trade secret offenses. *See* R29 Mtn., at 20–23. However, the defendant does not dispute that the Court's instructions to the jury accurately describe the elements of Counts Five and Six and the definition of "trade secrets." *See* Doc. 401, at 38–42. Indeed, the Court's instructions came directly from a joint submission by the parties. Doc. 399, at 4–6. Accordingly, the first step of the Court's analysis should be the trade secret law set forth in the instructions it gave to the jury,

not the defendant's post-trial spin on that law. The question before the Court is whether there was sufficient evidence before the jury — based on the law that it was given — from which it could conclude that the defendant committed the substantive trade secret offenses, and that he conspired to do so. As set forth in more detail below, the jury was presented with such evidence.

A. The Jury Was Presented with Sufficient Evidence from Which it Could Conclude That Korn/Ferry's Source Lists Constituted the Company's Trade Secrets.

The alleged trade secrets in this case were Korn/Ferry "source lists." Throughout his motion, Nosal challenges the conclusion that the government proved that any such source list was a trade secret. For example, he suggests that the jury could not have reasonably concluded that source lists were trade secrets because they may have contained information derived from public sources. *See, e.g.*, R29 Mtn., at 2, 19 & 25. Nosal also suggests that the jury could not have reasonably concluded that source lists were trade secrets because they "consist[ed] of nothing more than names, phone numbers, and company titles." *Id.* at 21–22; *id.* at 25 ("names are not trade secrets"). In addition, he argues that the government failed to prove that any of the source lists had not been disclosed to clients, sold as research, or brought to Korn/Ferry from another search firm. *See, e.g.*, *id.* at 31:10–23. As set forth below, however, the jury was presented with sufficient evidence from which it could conclude that the source lists taken from Korn/Ferry's computer system constituted "trade secrets" as defined under the law in Instruction 43.

1. *There Was Sufficient Evidence for the Jury to Conclude That Each Korn/Ferry Source List Constituted a Form and Type of Business Information in the Form of a Compilation.*

At trial, there was no confusion as to what a "source list" was. A "source list" was the list containing the names of, and other information pertaining to, the precise group of candidates that had been selected by Korn/Ferry employees to be presented to clients in specific Korn/Ferry search engagements (*i.e.*, assignments to fill a *particular* position at a *particular* company in a *particular* industry at a *particular* time). *See, e.g.*, RT 296:19–298:1, 299–300, 585:9–587:1 & 1094:17–21; *see also* RT 864:5–9 (source lists represented compendium of information). These lists were constructed by Korn/Ferry employees, based on their review of past source lists and additional research, as well as on the exercise of their judgment. RT 296:7–16, 299:3–12, 312:

20–313:5, 319:3–13, 340:16–20 & 1094:22–1095:17. After an engagement for a client was completed, the source list that had been developed by Korn/Ferry employees was maintained in Searcher and could be retrieved by employees working on other searches. RT 587:2–25.

Korn/Ferry's source lists clearly represented "forms and types of . . . business . . . information" in the form of "compilations." *See* Doc 401., at 42 (Instr. 43); 18 U.S.C. § 1839(3).

2. *There Was Sufficient Evidence for the Jury to Conclude That Korn/Ferry Took Reasonable Measures to Keep its Source Lists Secret.*

The government did not need to prove that Korn/Ferry took *all* conceivable measures to protect the secrecy of its source lists, or that the measures that the company adopted were perfect or foolproof. Rather, it had to prove only that the measures that Korn/Ferry took were reasonable under the circumstances. 142 *Cong. Rec.* S12201-03, at S12213 (1996) ("owners need not take heroic or extreme measures in order for their efforts to be reasonable"); *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003) ("The Act . . . does not require perfection."); *cf. Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1235–36 (8th Cir. 1994) ("The secrecy, however, need not be absolute. . . . Companies need not . . . create 'an impenetrable fortress.'"). Here, the jury was presented with evidence from which it could have concluded that Korn/Ferry took such reasonable measures to keep its source lists secret.

Briski testified about the physical and technological measures that Korn/Ferry implemented to protect the computer system containing source lists. *See, e.g.*, RT 583:11–584:11 (physical security of data center) & 584:13–585:8 (technological measures). And, as set forth in more detail in "The Evidence at Trial" Section, access to Korn/Ferry's computer system was not possible without a valid username and password. Moreover, Dunn testified that Korn/Ferry employees were required to enter into confidentiality agreements prohibiting them from disclosing source lists, *see, e.g.*, RT 356–57 & GX 7, and Nahas testified that source lists generally were not allowed to be sent outside of the company and given to non-Korn/Ferry employees. RT 298:5–7 & 304:15–16. Employees were required to return confidential information to the company upon termination of their employment. GX 7. Employees were also reminded of the proprietary and confidential nature of source lists whenever they exported a source list using Searcher's custom

report feature. *See* RT 615; GX 2, at 7 & 12.

The fact that Korn/Ferry made source lists available to employees both at the office and by remote access did not prevent the jury from finding that the company took reasonable measures to protect the secrecy of those source lists. The general importance of making source lists available to employees, and the good use that employees made of source lists for the benefit of the company, was well demonstrated at trial. *See* Section II.A.3, *infra*. In addition, the jury heard evidence that Korn/Ferry employees needed access to Searcher and the source lists in it at all times and at all places in order to do their jobs. RT 590:17–591:3.

Finally, the conclusion that Korn/Ferry had adopted reasonable measures is buttressed by the fact that, until it became aware of the offense conduct in May 2005, it had never discovered a theft of such magnitude, based on the "triggers" built into its system. RT 648–49; *see also* RT 616–17 (testimony re: choice of triggers to build). Once it discovered BC's and MJ's downloads prior to their departures from Korn/Ferry, Korn/Ferry took actions to retrieve the items that had been stolen and to strengthen its security measures through additional triggers. RT 649:8–19.

3. *There Was Sufficient Evidence for the Jury to Conclude That Source Lists Derived Actual or Potential Independent Economic Value from Not Being Generally Known To, and Not Readily Ascertainable Through Proper Means By, the Public.*

The jury also heard substantial evidence from which it reasonably could conclude that source lists derived independent economic value from not being generally known to, and not readily ascertainable through proper means by, the public.

There can be no serious dispute that source lists had economic value. Source lists from past searches were "frequently" retrieved and used in building source lists for new searches. RT 1095:6–17; *see also* RT 296:19–298:1 & 925:24–926:6. Witnesses testified as to the value of reviewing a prior source list when beginning a new source list related to an engagement to fill a similar position at a company in a similar industry. RT 893:11–22 & 897:5–898:6. Using prior source lists in this way gave Korn/Ferry employees a "springboard" and a "running start" with respect to new searches and helped Korn/Ferry to execute searches more quickly, which was something clients wanted. RT 301:10; *see also* RT 897:14–21 (use of prior source lists "leverages" prior searches), 920:24–921:14 (Nosal interested in "leveraging" names from prior

searches "to quickly bring candidates to fruition"), 886:22 (clients wanted searches to "be conducted in an expedient manner") & 954:10–11 (doing searches quickly "[m]akes the client very happy, and it opens the door to more searches"). Because prior source lists represented the results of Korn/Ferry employees' gleaning of suitable candidates from a multitude of source to create a compilation of information regarding a particular engagement, *see* RT 317:11–12 (source lists are "derived from years of accumulated work"), 340:24–3 (Searcher contains information "built for decades") & 1072–73 (BC testimony that Searcher information based on her review of many reference materials), those source lists had value from not being generally known to, and not being readily ascertainable through proper means by, the public.

The defendant's discussion of "customer lists" *qua* trade secrets is a red herring. *See* R29 Mtn., at 21. As he acknowledges, courts *have held* that "customer lists" may very well qualify as trade secrets. But even if courts had not so held, Korn/Ferry's source lists did not represent "[t]he list of customers to which a company sells its good or services." R29 Mtn., at 22:2. Source lists do not contain *customer* names (*i.e.*, the purchaser of work product), source lists contain *candidate* names (*i.e.*, the work product itself). Korn/Ferry's very delivery of its product was dependent on the source lists it developed. RT 586:22 (describing source lists as "the work product for the search"), 780:9–10 (describing source lists as "the work product of Korn/Ferry consultants to find executives for a particular position") & 863:20–25 ("Source lists are the work product for the engagements that Korn/Ferry does. It's the workpapers; it's the product . . . . The information that makes up the source list is the strategy . . . ."); *see also* RT 287:12–13 ("Our product is to identify, to assess and to recommend potential candidates to our clients.") & 378:2–9 ("identify, evaluate, and recommend superior candidates for leadership positions").

In addition to *identifying* executives appropriate for a particular search, source lists exported from Searcher could also contain information *about* the executives that was not generally known to, or readily ascertainable through proper means by, the public. For example, the jury heard that it was very important to have a cell, home, or direct line telephone number of a potential candidate. Search professionals spent a "considerable" amount of time on the telephone, RT 899–900, and there was great value in being able to be able to reach potential candidates

directly, without going through a gatekeeper. RT 914:18–21; *see also* RT 977:20 (cell, direct, and home numbers are "[e]xtraordinarily important") &1327:19–23 (cell/direct number "gets you around the gatekeeper"). Source lists viewed by the jury in this case, *see, e.g.*, GXs 58 & 59, contained such telephone numbers for many of the listed executives, information that the jury learned *was not* generally publicly available, RT 919:22–920:2.

There was also sufficient evidence for the jury to conclude that *none* of the source lists downloaded by BC and MJ had ever been disclosed to the public. *See* RT 977:21–25 (BC could not get April 2005 source lists anywhere else but from Korn/Ferry). Even though source lists might "rarely" be shared with a client, RT 300:25–301:4 & 345:15–23, Korn/Ferry did not make such lists available to the public or share them with competitors, RT 346:8–9 & RT 1095:21–24. Indeed, Briski testified that she had never seen any of these source lists publicly disclosed on the Internet, that the information in those source lists was created by Korn/Ferry employees, and that none of the source lists had ever been released by Korn/Ferry. RT 865:23–867:1.

For these reasons, the defendant's reliance on the facts that source lists may have contained some information derived from public sources or that such lists largely contained names and contact information for candidates ignores the fact that those lists represented Korn/Ferry's unique valuable compilation of a selected slice of information. That is all that is required. *Cf. Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994) ("a trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation") (pre-EEA case).[11]

---

[11] Although the defendant suggests that Korn/Ferry had stolen entire source lists, the evidence does not support that conclusion. The evidence before the jury was that Korn/Ferry employees developed the company's source lists for specific engagements that Korn/Ferry had been hired to conduct. *See also* GXs 198 & 199 (listing engagements pertaining to source lists); RT 975 (PerkinElmer and California Micro Devices source lists were related to searches done by Nosal at Korn/Ferry), 1018–19 (BC prepared source list for every search she did) & 1048:7–13 (source lists downloaded by BC were those she developed at Korn/Ferry).

B. Other Arguments Common to the Conspiracy and Substantive Offenses.

The defendant also raises two arguments that apply both to the conspiracy charge in Count One and to the substantive charges in Counts Five and Six. These arguments are the following:

- there was no proof that the alleged conspirators knew or firmly believed that the source lists were trade secrets, *see* R29 Mtn., at 26–28; *id.* at 31:24–32:5; *id.* at 33:9–10; and
- there was no evidence of the alleged conspirators' knowledge that the downloads would injure Korn/Ferry, *see id.* at 28–29; *id.* at 32:6–14.

As set forth below, the jury had sufficient evidence to make the requisite findings.

1. *There Was Sufficient Evidence from Which the Jury Could Conclude That Nosal, Christian, and Jacobson Knew or Firmly Believed That All of the Source Lists Taken from Korn/Ferry Were Trade Secrets.*

The defendant argues that the government failed to prove that Nosal, BC, and MJ knew or firmly believed that Korn/Ferry's source lists were trade secrets. This argument fails for several reasons. As an initial matter, with respect to the conspiracy charge, there was no need for the government to prove that the conspirators knew that the source lists that they intended to take and did take were actually trade secrets in order to establish the existence of a conspiracy. It was sufficient that they had a "firm belief" the source lists were trade secrets.

In any event, the government presented sufficient evidence upon which the jury could have reasonably concluded that Nosal, BC, and MJ *did know* that Korn/Ferry's source lists both were considered by Korn/Ferry to be trade secrets and were in fact trade secrets. The fact that Korn/Ferry may have shared *some* source lists with *clients* does not mean that those source lists became "generally known" or "readily ascertainable" to the *public*. And the fact that some Korn/Ferry search consultants, such as BC, may have *improperly* given source lists to people outside Korn/Ferry cannot support a finding that such source lists lost their trade secret status. *See* 18 U.S.C. § 1839(3)(b) ("proper means"); *United States v. Genovese*, 409 F. Supp.2d 253, 257 (S.D.N.Y. 2005) ("a trade secret does not lose its protection under the EEA if it is temporarily, accidentally or illicitly released to the public, provided it does not become 'generally known' or 'readily ascertainable through proper means'"); RT 1077 (provision of information to someone outside Korn/Ferry violated agreement to protect confidential information).

Indeed, if the source lists that were taken by BC and MJ *had* already become "generally known" and "readily ascertainable through proper means," there would have been no reason for BC and MJ to steal them from Korn/Ferry. The jury heard significant testimony, summarized above, as to why such source lists were valuable. The fact that the conspirators may have had some of the names from some of the lists in their BlackBerrys does not mean that the lists themselves were known or ascertainable. *See* RT 1227:10–1228:2 (not possible to put source lists or industry codes in BlackBerry); *see also* RT 1355:9–18 (Nosal's BlackBerry not big enough to hold information he wanted regarding potential candidates). And, certainly there would have been no reason for them to *conceal* their actions in doing so if the lists were generally known and readily ascertainable. *See, e.g.*, RT 614 (Searcher user had to check box to stop custom report title/format from being saved) & 631–32 (BC affirmatively checked box).

Nosal downplays the significant evidence that Korn/Ferry and its employees all understood that "source lists" represented the company's trade secrets. *See* R29 Mtn., at 27:16–28:2. However, in determining that the conspirators possessed the requisite knowledge, the jury could have reasonably relied on the confidentiality agreements that each of the conspirators signed in which they acknowledged that items such as source lists were "accorded the legal protection applicable to a company's trade secrets." *See* GX 7, at 1.

With respect to Nosal's own knowledge, at no time during his employment did he ever tell the company's chief legal officer, Peter Dunn, that he disagreed with any of the provisions in Korn/Ferry's confidentiality agreement. RT 359:20–360:2; *see also* RT 360:11–23 (same re: Nosal employment agreement). On the contrary, *Nosal*'s actions in requiring new hires to make acknowledgments regarding the trade secret status of source lists provide additional evidence of *his belief* that such materials were in fact trade secrets. *See* GX 15, at 3–4. The jury also could have relied on Nosal's surreptitious actions regarding the plans to take materials from Searcher to conclude that he knew that those items constituted valuable trade secrets that Korn/Ferry would not let him have. RT 1109–10 (MJ testimony that he "didn't want people to know" that he was taking materials from Korn/Ferry and agreeing that there was an "atmosphere of secrecy" from "the first moment that Mr. Nosal and I had a conversation"); *see also* RT 1285:2–5 ("[D]on't talk

about this in front of me. I don't want to hear it. Talk about it among yourselves."). In addition, when discussing how to transport the materials out of Korn/Ferry, Nosal instructed JFL to purchase computer media with his personal credit card, not his Korn/Ferry Diners Club card.[12] All of these actions on Nosal's part evince a belief that source lists were trade secrets.

The defendant notes that some of the witnesses never testified that they believed that source lists were "trade secrets." There was no requirement that they do so. Indeed, even if those witnesses had testified so, the Court instructed the jury that simply because a witness referred to information or documents as trade secrets "does not mean that they are necessarily trade secrets within the meaning of the statute." Doc. 401, at 43 (Instr. 44). The reverse of the coin is equally true; a witness's failure to label information or documents as a trade secret does not preclude trade secret status for that information or documents under the statute.

Finally, the defendant's argument that the conspirators had to "kn[o]w what constitute[d] a trade secret, as defined by federal law," R29 Mtn., at 19, is without merit. It is well established that ignorance of the law is no defense. The government need not prove that the conspirators had concluded that the information they were taking fit the legal definition of a "trade secret" in 18 U.S.C. § 1839(3). If the government had to prove this, Congress's intent would be contravened:

> For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is in fact proprietary. . . . This [knowledge] requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

142 *Cong. Rec.* S12201-03, at S12213 (1996). This legislative history confirms that the jury

---

[12] The defendant's argument that many "source lists" in Searcher were "brought to KFI by new hires," R29 Mtn., at 27–28, demonstrates a misunderstanding of what a "source list" was and what BC and MJ took. As set forth above, Korn/Ferry "source lists" represented compilations of information put together by its search consultants with respect to engagements that *Korn/Ferry* did. As BC testified, the source lists that she obtained were not brought to Korn/Ferry by new hires, but were related to searches that Nosal and other Korn/Ferry search consultants had done at Korn/Ferry. RT 933:4–8; *see also* RT 1018:24–1019:1 (BC prepared source list for every search she did), 1048:7–13 (source lists downloaded by BC were those she developed at Korn/Ferry) & 1108:1–6 (MJ: "I took examples of search work that I had been responsible for working on . . . . that would include source lists . . . .").

could conclude that the conspirators knew that the source lists were trade secrets because they were protected by proprietary markings, security measures, and confidentiality agreements. More generally, the jury could conclude that the conspirators knew that the information was valuable to Korn/Ferry because it was not generally known to the public, and that Korn/Ferry had taken reasonable measures to protect it.

Based on all of the above, the jury reasonably could have concluded that the conspirators knew that the source lists at issue were trade secrets.

2. *There Was Sufficient Evidence from Which the Jury Could Conclude That Nosal, Christian, or Jacobson Intended or Knew That the Theft of Korn/Ferry's Trade Secrets Would Injure Korn/Ferry.*

The jury could also have reasonably concluded that the conspirators intended or knew that their actions would injure Korn/Ferry.[13]

As an initial matter, the jury heard considerable evidence that the executive search industry is a "highly competitive" one and that firms compete vigorously for clients. *See* RT 290:15–292:11 & 889:4–17. Both BC and MJ recognized that it was a competitive industry. RT 916:17–917:4 & 1201:1–2.

Dunn also testified that, along with its people, the database that contained source lists (Searcher) was a "core asset" of the company, and that the company spent millions of dollars per year to improve and maintain its data resources. RT 350:11–24. This information was communicated to employees like Nosal, BC, and MJ. *See, e.g.*, GX 7, at 1 ("K/F has made substantial investments in new technology to make these information databases more readily available to its personnel . . . ."); *cf. also* GX 6, at 6 (Code of Business Conduct directive to "[p]rotect the Company's assets . . .").

Nahas testified that, if a Korn/Ferry competitor obtained a Korn/Ferry source list regarding a relevant search, "they'd have a competitive advantage from the standpoint that they'd have

---

[13] In his motion, the defendant suggests that the government had to prove "knowledge of, *and* intent to inflict, injury." R29 Mtn., at 28:16–18 (emphasis added). However, the law allows conviction where either of these facts are proved. *See* 18 U.S.C. § 1832(a) ("intending or knowing"); Doc. 401, at 38 ("the defendant knew or intended") (Instr. 40).

information that they wouldn't have had otherwise, which could be used in a competitive situation. It could enable them to do better at a search, which could have impact on a competitor," such as Korn/Ferry. RT 304:18–25; *see also* RT 305:1–11 (Nahas testimony that competitor's possession of Korn/Ferry source list would give it "a running start"). For these reasons, Nahas testified that she had never given a source list to a competitor. RT 346; RT 1095 (same re: MJ).

Based on the competitiveness of the executive search industry, the efforts that Korn/Ferry took to protect the confidentiality of information in Searcher, the efforts to which the conspirators went to steal that information, and Nosal's, BC's, and MJ's extensive experience in the executive search industry and at Korn/Ferry, the jury reasonably could have concluded that the conspirators intended or knew that the theft of information from Korn/Ferry for use in Nosal's competing executive search activities would injure Korn/Ferry. *Cf. also* RT 1078 (BC testimony that settling with Korn/Ferry and paying it money was "the right thing to do" because "that was Korn/Ferry's information and it belonged to the company").

Moreover, the jury was presented with other evidence from which it could have concluded that Nosal intended that there would be injury to Korn/Ferry. For example, the defendant's personal animus toward Korn/Ferry was well demonstrated. BC testified that Nosal was "furious" that Bob Damon had been named President of Korn/Ferry North America instead of Nosal. RT 928–29; *see also* RT 950–51 (describing Nosal as "livid"). It was after Nosal was passed over for this promotion that he decided to leave Korn/Ferry, start his own business to compete with Korn/Ferry, and to take materials from Korn/Ferry.

Nosal's personal animus toward Korn/Ferry was further demonstrated by his orchestration of BC's "resignation" e-mail, which was introduced as DX R. BC testified that Nosal helped her dictate that e-mail, wrote part of it, and encouraged her to leave Korn/Ferry "because he was interested in creating kind of a fireball effect from his departure." RT 1067. BC also testified that Nosal had become "very angry" when he had been "called out" by his superiors at Korn/Ferry about having an improper relationship with BC, one of his subordinates. RT 1068–69.

Moreover, BC testified that after Nosal left Korn/Ferry he expressed no reservations about taking materials from Korn/Ferry because he believed that they belonged to him. RT 949:17–19;

see also RT 977:2 ("he was not concerned about Korn/Ferry"). Nosal pressured BC to give those materials to him so that he could use them to populate the Encore database product that he had purchased from Cluen Corporation, RT 949–50, and, with respect to the April 2005 source lists, actually received materials from BC for use in two searches. One of those searches (UTStarcom) was for a Korn/Ferry client. *See* GX 10, at 1.

Based on all of these facts, the jury reasonably could have concluded that Nosal intended or knew that his actions would injure Korn/Ferry. Further, because BC knew all of these same facts, her agreement to participate in the conspiracy to take materials from Korn/Ferry is evidence upon which the jury could rely to conclude that she possessed the requisite intent or knowledge that the conspiracy's actions would injure Korn/Ferry.

Nosal's argument regarding the availability of the downloaded information on "Hoover's," R29 Mtn., at 28:23–25, again ignores the evidence that "source lists" represented compilations regarding individuals that Korn/Ferry search consultants believed were good candidates for particular positions and particular companies in particular companies. Further, despite the defendant's statement to the contrary, the evidence does not support the conclusion that *source lists* "were commonly brought from one executive search firm to another and exchanged with friends." R29 Mtn., at 28:25–27. Even though BC provided unspecified "stuff" from Korn/Ferry to friends outside of Korn/Ferry, the testimony was clear that this was improper and not done with Korn/Ferry's permission. *See* RT 916:24–917:4, 1019–20 & 1076:15–1077:7. Nosal's argument that "neither BC nor MJ testified that they 'made any use' of the materials they downloaded while at KFI," R29 Mtn., at 28–29, ignores the testimony to the contrary. For example, BC testified that she *did* use the materials in searches that she did with the defendant. RT 949:4–9. Further, MJ certainly put the materials that he took "to use" in the sense that he was working to get that information into Nosal's new database. RT 1136:21–1138:24; *see also* RT 933:4–8 (BC testimony that Nosal wanted her to obtain things that "would be helpful for him to quickly utilize for his business"), 1105:6–10 (MJ understanding that one of his tasks for Nosal's new company "would be bring information from Korn/Ferry over"), 1135:22–23 (Encore database empty when purchased) & 1146:9–1149:14 (MJ discussing efforts to get Korn/Ferry data and other

information into Encore in order to "re-create Searcher"). Once in Nosal's database, those materials would be used to compete against Korn/Ferry.

C. There Was Sufficient Evidence to Find Nosal Guilty of the Trade Secret Conspiracy.

The defendant argues that there was insufficient evidence for the jury to conclude that he was guilty of the trade secret conspiracy charged in Count One. In addition to the arguments that he raises that are applicable to both the conspiracy and the substantive trade secret offenses, *see* Sections I.A–B, *supra*, the defendant makes the following arguments as to the conspiracy charge:

- there was no proof as to the specific content of source lists downloaded before April 12, 2005 and no proof that any of those source lists met the definition of "trade secret," R29 Mtn., at 25–26;
- all of the pre-April 2005 source lists were obtained by alleged conspirators who were "authorized to download and obtain the information," *id.* at 29;
- there was no proof that the defendant received any of the pre-2005 source lists, or that there was agreement that he would receive them, *id.* at 29–30; and
- the downloading of information and source lists in June and July 2005 was not evidence upon which the jury could rely to conclude that there was a trade secret conspiracy, *id.* at 33–34.

As set forth in Sections II.C.1–3, *infra*, these arguments are without merit and do not compel a judgment of acquittal with respect to Count One.

1. *Setting Aside the Pre-April 2005 Source Lists and the June and July Downloads, The Events of April 2005 Presented Sufficient Evidence upon Which the Jury Could Conclude That Nosal Was Guilty of Conspiracy.*

In the part of his brief seeking acquittal on the conspiracy charge, the defendant focuses almost entirely on the source lists that were obtained by alleged conspirators Christian and Jacobson before April 2005 (the "pre-April 2005 source lists") and the information and source lists downloaded in June and July 2005. Missing from his conspiracy discussion is a consideration of the evidence presented to the jury regarding Nosal's instructions to Christian to download source lists from Searcher in April 2005 for the UTStarcom and WorldHeart searches.

The evidence regarding the events in April 2005 is set out at pages 6–8 and 21–24, *supra*. As set forth more fully therein, Nosal specifically directed Christian to get source lists from Korn/Ferry engagements from Searcher. *See, e.g.*, RT 959:19–960:13. From this evidence alone, the jury reasonably could have found Nosal guilty of conspiring to steal trade secrets.

BC's e-mailing of those source lists to Nosal also constituted sufficient evidence upon which the jury could conclude that Nosal conspired to receive and possess stolen trade secrets. *See* GX 58 & 60. Although there was no computer metadata regarding whether Nosal had opened the attachment to one of the e-mails that contained three source lists (*i.e.*, GX 58), the jury reasonably could have concluded that he *did* open it and examine its contents. After all, Nosal had asked BC to obtain those source lists for him for use with respect to a specific client, UTStarcom. It would be strange to conclude that, after having asked BC to *get* the source lists, Nosal declined to look at them, especially in light of the fact he and BC at the time were trying to *get* UTStarcom's business. Furthermore, names from those source lists were later presented by Nosal and BC as potential candidates to UTStarcom. In addition, a copy of one of the source lists in GX 58 — bearing handwriting that was *not* Christian's — was found in her apartment, a place where Nosal performed work. *See* GX 59. Finally, a copy of one of the e-mails in GX 60 was also found in Christian's apartment, covered in Nosal's handwriting. *See* GX 63.

For these reasons, based solely on the evidence regarding the events in April 2005, the jury reasonably could have found Nosal guilty of conspiracy to steal, receive, and possess trade secrets belonging to Korn/Ferry. Accordingly, the defendant's specific arguments regarding the pre-April 2005 source lists and the June and July downloads do not undermine the jury's verdict.

2. *The Defendant's Specific Arguments Regarding the Pre-April 2005 Source Lists are Without Merit.*

As set forth above, the jury was presented with sufficient evidence regarding the events of April 2005 from which it could have reasonably concluded that Nosal was guilty of the trade secret conspiracy. In addition, the jury could also have relied on the evidence regarding Nosal's direction to his conspirators to take source lists and other items from Korn/Ferry before April 2005 to conclude that such a conspiracy existed. Despite the defendant's protestations to the contrary, R29 Mtn., at 26:6–7, the evidence regarding the pre-April 2005 source lists had *enormous* "probative value as to the Count One conspiracy charge."

/ //

/ / /

i. The Jury Did Not Require Proof as to the "Specific Content" of the Pre-April 2005 Source Lists to Conclude That There Was a Conspiracy, Nor Did it Require Proof That Any of the Pre-April 2005 Sources Lists Met the Definition of Trade Secret.

The defendant argues that the jury could not rely on the evidence regarding Christian's and Jacobson's downloads of source lists while they were still employed at Korn/Ferry in finding the existence of a conspiracy because the government proved neither the content of those lists nor that the lists were trade secrets. The government did not have this burden.

Nosal was charged in Count One with *conspiring* to misappropriate, receive, possess, and transmit trade secrets. Under the law, the government was not required to prove either that any trade secret was actually misappropriated, received, possessed, or transmitted or that the source lists that were the target of the conspiracy were in fact trade secrets. *See United States v. Yang*, 281 F.3d 534, 544 (6th Cir. 2002) ("legal impossibility" is not a defense to prosecution for conspiring to steal trade secrets); *United States v. Hsu*, 155 F.3d 189, 203 (3d Cir. 1998) (same); Doc. 401, at 46 (Instr. 47) ("the government need not prove the existence of actual trade secrets and that Defendant knew that the information in question was a trade secret"). Here, the jury was presented with sufficient evidence regarding Christian's and Jacobson's downloads in 2004 and early 2005 from which it could conclude that the defendant conspired to misappropriate, receive, possess, or transmit source lists belonging to Korn/Ferry.

In any event, there was sufficient evidence for the jury to conclude that Korn/Ferry's source lists met the legal definition of "trade secret." It was undisputed that materials designated by Korn/Ferry as "source lists" were among the materials that Christian and Jacobson downloaded on various dates in August, September, and December 2004 and in January and February 2005. *See* GXs 22 & 23; *see also* RT 933:1–8 & 936:16–937:3. Given the significant testimony about what source lists were, *see* Section II.A, *supra*, the jury did not need to be shown the specific content of any lists for it to conclude that they were trade secrets.

The jury could also have reasonably concluded from the evidence that the source lists downloaded by BC and MJ in 2004 or early 2005 had not been disclosed to the public, thereby becoming "generally known" and "readily ascertainable through proper means." Also, as noted above, if any of the source lists taken by BC and MJ had become "generally known" or "readily

ascertainable," there would have been no reason for them to steal those source lists and to hide their actions from Korn/Ferry.

ii. *The Jury Reasonably Could Have Concluded that BC and MJ Lacked Authorization to Download Source Lists with the Intent to Steal Them for Non-Korn/Ferry Business, And to Take Such Materials When They Left Korn/Ferry.*

Nosal argues that there was "no proof" that BC and MJ "lacked authorization" to download source lists prior to their resignations. *See* R29 Mtn., at 29. The defendant's argument in this regard, however, confuses "authorization" to access a computer, with authorization to take certain actions pertaining to trade secrets. In a nutshell, the defendant argues that, because BC and MJ were authorized to *access* Korn/Ferry's computer system during their employment, they could not be liable under 18 U.S.C. § 1832 for downloading, copying, and duplicating trade secrets in that computer system. However, it would render the trade secret law entirely toothless to adopt the defendant's reading of it. The fact that Korn/Ferry employees with valid usernames and password may have been authorized to access "every nook and cranny of Searcher" does not mean that they were authorized to misappropriate, download, duplicate, or copy information from Searcher without permission for a non-Korn/Ferry use under the trade secret statute. The defendant made this very argument during closing, RT 1651:15–19, and the jury rejected it.

Indeed, the Ninth Circuit in its en banc decision in this case recognized that, while "misappropriation" was not covered by the CFAA, it was *certainly* covered by the trade secrets statute. *Nosal*, 676 F.3d at 857 & n.3. There can be no serious dispute in this case that Korn/Ferry placed restrictions on its employees' misappropriation of its trade secrets through its confidentiality agreements, computer banners, and computer warnings and that the conspirators were without authorization to take for their own use any trade secrets belonging to Korn/Ferry. *See, e.g.*, GXs 7, 9 (at p.9), 12, 13 (at p.4), 14, 15 (at pp.3–4), 16 & 17 (at p.4).

In any event, the defendant's motion focuses only on authorization to "download, duplicate, or copy" trade secrets. *See* R29 Mtn., at 29. Even if the computer access rights granted to BC and MJ allowed them to take *those* actions, their access rights certainly did not allow them to do such things as "appropriate," "take," "carry away," or "conceal by fraud, artifice, and deception" any trade secrets. *See* Doc. 401 (Instrs. 40, 41, 48). There was abundant evidence that

both BC and MJ downloaded source lists from Korn/Ferry's computer system and then took those items with them when they left Korn/Ferry. RT 936:12–937:8 & 1107:22–1108:19.

iii. *The Jury Did Not Require Proof That Nosal Actually Received the Trade Secrets That Were Stolen Before April 2005 for it to Conclude That There Was a Trade Secret Conspiracy.*

At trial, the jury learned that Nosal specifically told BC to take source lists from Searcher that he could use in his new business, and that BC did so. RT 933:1–8 & 936:16–937:3. The jury also learned that MJ took source lists from Korn/Ferry based on his discussions with Nosal to obtain materials that would be useful for Nosal's new business. RT 1107–08. BC testified that she used some of the materials in searches that she conducted with Nosal after she left Korn/Ferry, RT 949:4–9, and MJ testified that he was working to get stolen materials into Nosal's new database. Further, the jury heard from JFL that Nosal authorized her to purchase computer media onto which to copy materials from Korn/Ferry's computer system. *See* GXs 131 & 157; RT 1286–1289:4. This was more than enough evidence from which the jury could conclude that there was an agreement between Nosal, BC, MJ, and JFL to take materials from Korn/Ferry.

BC testified that the defendant began asking her for the materials that she had stolen from Korn/Ferry "[p]retty soon after he was putting all the pieces together for his new business, and, also when he realized that [she] was ending the relationship." BC testified that those "pieces" were not together until at least May 2005, but perhaps as late as July 2005. RT 950:4–22; RT 924 (relationship ended in spring 2005). Although BC may have decided at a later time to *not* give the materials that she had taken to Nosal, that does not mean that a conspiracy was not proven with respect to her initial theft. Further, both MJ and JFL testified that it was their understanding that Nosal wanted them to take materials from Korn/Ferry's computer system, and they each took actions indicating their agreement to do so. RT 1105:6–10, 1108:1–19 & 1292:13–23. Nosal knew that MJ was working on getting those materials into Nosal's new database in July 2005.

3. *The Jury Could Have Relied on the Downloading of Source Lists in July 2005 as Further Evidence of a Conspiracy.*

Finally, the defendant argues that the jury could not have reasonably relied on any source list downloads in July 2005 to find the existence of a conspiracy. *See* R29 Mtn., at 33–34.

The defendant first argues that, because Korn/Ferry was aware that JFL "was using her password to facilitate downloads of Searcher information for non-KFI purposes," Korn/Ferry did not take "reasonable measures." This argument, however, ignores the fact that the defendant was charged with *conspiracy* in Count One. The fact that Korn/Ferry may have suspected that JFL was misappropriating trade secrets does not absolve the conspirators of liability for conspiring to steal trade secrets. In any event, the evidence did not support the conclusion that "KFI deliberately decided to permit [the July 2005] material to be made public." R29 Mtn., at 19:20. Peter Dunn testified that he believed that he knew where the stolen data had been taken, and that those who had taken it were not going to make it public, but, rather, were going to maintain its secrecy and use it for their own benefit. RT 1507. Indeed, Christian's testimony was that she took the materials from Korn/Ferry's computer system for use in Nosal's new business, RT 985–86, making it unlikely she would not disclose the materials to Nosal's competitors.

The defendant also argues that there was insufficient proof as to what was downloaded by BC on July 12 and by MJ on July 29. R29 Mtn., at 34:17–28. Although BC did not remember obtaining it, the evidence was clear that a source list for the Duke Energy engagement was obtained and exported on July 12, *see* 694–95, and the jury saw the re-creation of that source list based on Korn/Ferry's logs. *See* GX 43, at 3–6. With respect to the source lists obtained on July 29, it does not matter to the question of the trade secret conspiracy that Korn/Ferry may have "already brought federal investigators onto the scene." R29 Mtn., at 34:25–26. Moreover, the government introduced undisputed evidence that Jacobson downloaded 25 Korn/Ferry source lists that day. RT 701. The government also introduced Korn/Ferry's audit of the source list custom reports that were run on July 29. GX 47; RT 743–44. There was significant testimony regarding source lists throughout the trial, and there was no need for the government to present any additional evidence regarding any of the source lists obtained on July 12 and July 29 for the jury to conclude that the efforts to obtain them were relevant to the trade secret conspiracy.[14]

[14] The government agrees that the downloads in June 2005 were not of source lists, and the government's theory at trial was only that source lists constituted trade secrets.

D. There was Sufficient Evidence from Which the Jury Could Find Nosal Guilty of the Substantive Trade Secret Counts.

For the same reasons that the Court should uphold the defendant's conspiracy conviction, it should also uphold his convictions for the substantive counts in Counts Five and Six. The government has already addressed the defendant's specific arguments regarding the substantive trade secret counts in Sections II.A–B, *supra*, and will not repeat those arguments here. As set forth in more detail in those sections, there was sufficient evidence from which the jury could conclude that the four source lists at issue in Counts Five and Six were "trade secrets" as defined in 18 U.S.C. § 1839(3), that Nosal and BC knew that the source lists were trade secrets, and that Nosal and BC intended or knew that their actions would injure Korn/Ferry. As set forth in Section I.C.1, *supra*, there was substantial evidence that Nosal directed BC to obtain the source lists identified in Counts Five and Six from Korn/Ferry to assist in the UTStarcom and WorldHeart searches in April 2005. Immediately after he directed her to take those actions, he received e-mails from her containing information relevant to those searches.[15]

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

[15] Even if the evidence of Nosal's direction to Christian to obtain these materials from Korn/Ferry was insufficient for the jury to conclude that Nosal was guilty of Counts Five and Six under an aiding and abetting theory, the jury could nevertheless have found him guilty of these counts under a *Pinkerton* theory, for the same reasons that it could have found him guilty of the CFAA counts. *See* Section I.D, *supra*.

CONCLUSION

For all of the reasons stated above, the United States respectfully requests that the Court deny the defendant's Motion for Acquittal Under Rule 29 in its entirety.

DATED: July 12, 2013

Respectfully submitted,

MELINDA HAAG
United States Attorney

/s/
KYLE F. WALDINGER
MATTHEW A. PARRELLA
Assistant United States Attorneys

/s/
JENNY C. ELLICKSON
Trial Attorney